|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

**ЛЕКЦИОННЫЕ МАТЕРИАЛЫ**

|  |  |
| --- | --- |
| **Основы информационной безопасности** | |
| *(наименование дисциплины (модуля) в соответствии с учебным планом)* | |
| Уровень | бакалавриат, специалитет |
|  | *(бакалавриат, магистратура, специалитет)* |
| Форма обучения | очная |
|  | *(очная, очно-заочная, заочная)* |
| Направление(-я)  подготовки | 10.03.01 «Информационная безопасность», 10.05.03 «Информационная безопасность автоматизированных систем» |
|  | *(код(-ы) и наименование(-я))* |
|  |  |
| Институт | комплексной безопасности и специального приборостроения (ИКБСП) |
|  | *(полное и краткое наименование)* |
| Кафедра | Защита информации (КБ-1) |
|  | *(полное и краткое наименование кафедры, реализующей дисциплину (модуль))* |
| Лектор | Вершинин Александр Николаевич |
|  | *(сокращенно – ученая степень, ученое звание; полностью – ФИО)* |

|  |  |  |  |
| --- | --- | --- | --- |
| Используются в данной редакции с учебного года | 2020/21 | | |
|  | *(учебный год цифрами)* | | |
| Проверено и согласовано «\_\_\_\_» \_\_\_\_\_\_\_\_20\_\_\_г. |  |  |  |
|  | *(подпись директора Института/Филиала с расшифровкой)* | | |

Москва 20\_\_ г.

**Конспект лекций**

**Введение.**

Курс дисциплины «Основы информационной безопасности» ведет **Вершинин Александр Николаевич**.

Курс построен в соответствии с требованиями федеральных государственных образовательных стандартов по направлениям 10.03.01 «Информационная безопасность», 10.05.03 «Информационная безопасность автоматизированных систем» и рабочей программой дисциплины «Основы информационной безопасности»

В современном мире информация становится стратегическим ресурсом. Быстрое совершенствование информатизации в России, проникновение ее во все сферы жизненно важных интересов личности, общества и государства вызвали помимо несомненных преимуществ и появление ряда существенных проблем. Одной из них стала необходимость защиты информации. Учитывая, что в настоящее время потенциал страны все в большей степени определяется уровнем развития информационной структуры, пропорционально растет потенциальная уязвимость от информационных воздействий.

Распространение компьютерных систем, объединение их в коммуникационные усиливает возможности электронного проникновения в них.

Проблема компьютерной преступности во всех странах мира, независимо от их географического положения, вызывает необходимость привлечения все большего внимания и сил общественности для организации борьбы данным видом преступлений. Особенно широкий размах получили преступления в автоматизированных банковских системах и в электронной коммерции.

Хотя уровень внедрения новейших информационных технологий в практику в России не столь значителен, компьютерные преступления с каждым днем дают о себе знать все более и более, а защита государства и общества от них превратилась в суперзадачу для компетентных органов.

Одной из основных причин, связанных с компьютерами, является недостаточная образованность в области безопасности. Только наличие некоторых знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление или своевременно обнаружить подозреваемого.

В связи с этим, основной задачей преподавания дисциплины «Основы информационной безопасности» является подготовка кадров, обладающих знаниями, навыками, умениями, в сфере обеспечения информационной безопасности организаций различных форм собственности.

Целью учебного курса является формирование профессиональной компетентности на основе системы теоретических и методологических знаний и специальных умений в области информационной безопасности и их использования в профессиональной деятельности будущего специалиста.

Развитие теории информационной безопасности в настоящее время связано с учетом новых обстоятельств, характерных для современного периода развития информатизации общества.

В объеме курса предусмотрено проведение лекций (32 часов), практических занятий (16 часов).

Контроль знаний обучаемых осуществляется в ходе сдачи зачета.

В случае, если входе обучения будут возникать какие-либо вопросы к лектору, их можно направлять по электронной почте по адресу ve.sa.2009@mail.ru.**Раздел 1. Основные понятия и задачи информационной безопасности. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности. Стандарты информационной безопасности.**

Изучению основ информационной безопасности должно предшествовать изучение курса информатики, где объясняется сам термин «информации»(от латинского informatio— «научение», «сведение», «оповещение»). В целях замкнутости изложения напомним некоторые сведения, которые будут использоваться далее.

Что такое «информация»? Ответить достаточно сложно.

На обще лексическом, бытовом уровне понятие «информация» обычно толкуется как «сообщение, осведомляющее о положении дел, о состоянии чего-нибудь». Заметим, что и в нормативных правовых актах чаще всего данное понятие употребляется именно в этом смысле. [Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. — М., 1992. С. 255.]

Норберт Винер (1894-1964) определял информацию как «обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления». Он же говорил, что «информация есть информация, а не материя и не энергия».

Можно встретить и более глубокий подход к информации, как «опосредованный формами связи результат отражения изменяемого объекта изменяющимся с целью сохранения их системной целостности» (см. например, Википедия).

Информация первична и содержательна - это категория, поэтому в категориальный аппарат науки она вводится описанием, через близкие категории: материя, система, структура, отражение. С информацией связаны понятия – знание, данные, сигналы, сообщения, смысл, семантика. Не следует путать категорию информация с понятием знание. Знание определяется через категорию информация.

В материальном мире человека информация материализуется через свой носитель и благодаря ему существует. Сущность материального мира предстаёт перед исследователем в единстве формы и содержания. Передаётся информация через носитель. Материальный носитель придаёт информации форму. В процессе формообразования производится смена носителя информации.

В ХХ веке слово «информация» стало термином во множестве научных областей, получив особые для них определения и толкования.

Чтобы зафиксировать термин для дальнейшего обращения с ним воспользуемся Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Итак,

«**информация** - сведения (сообщения, данные) независимо от формы их представления».

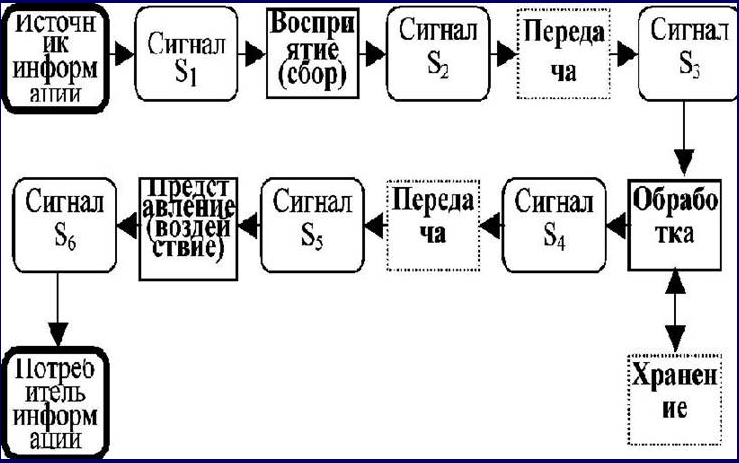
В общем, это согласуется с трактовкой информации в справочной философской литературе последнего времени как «одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.».

Интересно отметить, что в отмененном Законе от 1995 г. «Об информации, информатизации и защите информации» указывалось, что «информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления». Как видим, старое определение хуже, перечисление страдает существенной неполнотой.

Приведем и некоторые другие понятия, связанные с термином «информация», из нового закона.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационные процессы** - процессы, связанные с поиском, хранением, передачей, обработкой и использованием информации, называются информационными процессами.



### ЗАЩИТА ИНФОРМАЦИИ

### Теперь остановимся на основных информационных процессах.

**1. Поиск.**

***Поиск информации -*** это извлечение хранимой информации.   
Методы поиска информации:

 непосредственное *наблюдение;*

 *общение* со специалистами по интересующему вас вопросу;

 *чтение* соответствующей литературы;

 *просмотр* видео, телепрограмм;

 *прослушивание* радиопередач, аудиокассет;

 работа в библиотеках и архивах;

 *запрос* к информационным системам, базам и банкам компьютерных данных;

 другие методы.

Понять, *что* искать, столкнувшись с той или иной жизненной ситуацией, осуществить процесс поиска - вот умения, которые становятся решающими на пороге третьего тысячелетия.

**2. Сбор и хранение.**

Сбор информации не является самоцелью. Чтобы полученная информация могла использоваться, причем многократно, необходимо ее хранить.   
***Хранение информации -*** это способ распространения информации в пространстве и времени.

Способ хранения информации зависит от ее носителя *(книга- библиотека, картина- музей, фотография- альбом).* ЭВМ предназначен для *компактного хранения* информации с возможностью *быстрого доступа* к ней.

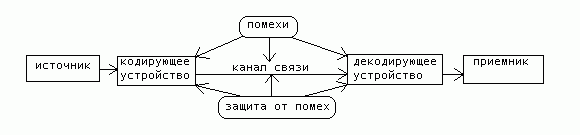
***Информационная система -*** это хранилище информации, снабженное процедурами ввода, поиска и размещения и выдачи информации. Наличие таких процедур- главная особенность информационных систем, отличающих их от простых скоплений информационных материалов. *Например, личная библиотека, в которой может ориентироваться только ее владелец, информационной системой не является. В публичных же библиотеках порядок размещения книг всегда строго определенный. Благодаря ему поиск и выдача книг, а также размещение новых поступлений представляет собой стандартные,* ***формализованные*** *процедуры.*

**3. Передача.**

В процессе передачи информации обязательно участвуют *источник* и *приемник* информации: первый передает информацию, второй ее получает. Между ними действует канал передачи информации - *канал связи.*   
 ***Канал связи -*** совокупность технических устройств, обеспечивающих передачу сигнала от источника к получателю.

***Кодирующее устройство -*** устройство, предназначенное для преобразования исходного сообщения источника к виду, удобному для передачи.   
 ***Декодирующее устройство -*** устройство для преобразования кодированного сообщения в исходное.

Деятельность людей всегда связана с передачей информации.   
В процессе передачи информация может теряться и искажаться: искажение звука в телефоне, атмосферные помехи в радио, искажение или затемнение изображения в телевидении, ошибки при передачи в телеграфе. Эти помехи, или, как их называют специалисты, шумы, искажают информацию. К счастью, существует наука, разрабатывающая способы защиты информации - ***криптология.***



Каналы передачи сообщений характеризуются *пропускной способностью* и *помехозащищенностью.*

Каналы передачи данных делятся на *симплексные* (с передачей информации только в одну сторону (телевидение)) и *дуплексные* (по которым возможно передавать информацию в оба направления (телефон, телеграф)). По каналу могут одновременно передаваться несколько сообщений. Каждое из этих сообщений выделяется (отделяется от других) с помощью специальных фильтров. Например, возможна фильтрация по частоте передаваемых сообщений, как это делается в радиоканалах. **Пропускная способность канала** определяется максимальным количеством символов, передаваемых ему в отсутствии помех. Эта характеристика зависит от физических свойств канала.

Для повышения помехозащищенности канала используются специальные методы передачи сообщений, уменьшающие влияние шумов. Например, вводят лишние символы. Эти символы не несут действительного содержания, но используются для контроля правильности сообщения при получении.   
С точки зрения теории информации все то, что делает литературный язык красочным, гибким, богатым оттенками, многоплановым, многозначным,- избыточность. Например, как избыточно с таких позиций письмо Татьяны к Онегину. Сколько в нем информационных излишеств для краткого и всем понятного сообщения "Я Вас люблю!"

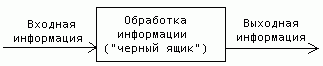
**4. Обработка.**

*Обработка информации -* преобразование информации из одного вида в другой, осуществляемое по строгим формальным правилам.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Примеры обработки информации** | | | | | | | |
| ***Примеры*** | ***Входная информация*** | ***Выходная информация*** | ***Правило*** |  |  |  |  |
| Таблица умножения | Множители | Произведение | Правила арифметики |  |  |  |  |
| Определение времени полета рейса "Москва-Ялта" | Время вылета из Москвы и время прилета в Ялту | Время в пути | Математическая формула |  |  |  |  |
| Отгадывание слова в игре "Поле чудес" | Количество букв в слове и тема | Отгаданное слово | Формально не определено |  |  |  |  |
| Получение секретных сведений | Шифровка от резидента | Дешифрованный текст | Свое в каждом конкретном случае |  |  |  |  |
| Постановка диагноза болезни | Жалобы пациента + результаты анализов | Диагноз | Знание + опыт врача |  |  |  |  |

Обработка информации по *принципу "черного ящика" -* процесс, в котором пользователю важна и необходима лишь входная и выходная информация, но правила, по которым происходит преобразование, его не интересуют и не принимаются во внимание.

**"Черный ящик"** - это система, в которой внешнему наблюдателю доступны лишь информация на входе и на выходе этой системы, а строение и внутренние процессы неизвестны.



**5. Использование.**

Информация используется при принятии решений.

 Достоверность, полнота, объективность полученной информации обеспечат вам возможность принять правильное решение.

 Ваша способность ясно и доступно излагать информацию пригодится в общении с окружающими.

 Умение общаться, то есть обмениваться информацией, становится одним главных умений человека в современном мире.   
**Компьютерная грамотность** предполагает:

 знание назначения и пользовательских характеристик основных устройств компьютера;

 Знание основных видов программного обеспечения и типов пользовательских интерфейсов;

 умение производить поиск, хранение, обработку текстовой, графической, числовой информации с помощью соответствующего программного обеспечения.   
**Информационная культура пользователя включает в себя:**

 понимание закономерностей информационных процессов;

 знание основ компьютерной грамотности;

 технические навыки взаимодействия с компьютером;

 эффективное применение компьютера как инструмента;

 привычку своевременно обращаться к компьютеру при решении задач из любой области, основанную на владении компьютерными технологиями;

 применение полученной информации в практической деятельности.

**6. Защита.**

**Защитой** информации называется *предотвращение:*

 *доступа* к информации лицам, не имеющим соответствующего разрешения (несанкционированный, нелегальный доступ);

###  непредумышленного или недозволенного *использования, изменения* или *разрушения* информации.

### Более подробно о защите информации мы остановимся далее. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

**Обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

**Доступ к информации** - возможность получения информации и ее использования.

**Электронное сообщение** - информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

(иногда можно встретить термин **«компьютерная информация»** - информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ [Комментарии к УК РФ. Под ред. Скуратова Ю.И. и Лебедева В.М. М.: НОРМА, 1996-832 с.])

**Документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Особо можно выделить понятие

**Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В качестве комментария можно заметить, что это только часть возможных требований или свойств, которые возможны. Например, как будет подчеркнуто далее, можно выделить «целостность информации», «доступность информации» и другое.

Продолжая перечень понятий, выделим из [ГОСТ Р 50922 -96 ] понятие:

**защищаемая информация** – «информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми **собственником информации».**

Однако теперь по№ 149-ФЗ [ Об И, ИТ и о ЗИ] к собственнику информации добавился еще и обладатель информации, защищающий ее ограничением доступа, как сказано в определении**.**

**В новом законе** № 149-ФЗ понятие защищаемая информация отсутствует, хотя в старом законе оно было, и говорилось, что «**защищаемая информация** – любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу». По-видимому, решили убрать ограничение, связанное с документированностью информации.

Согласно ФЗ № 149-ФЗ, информация в зависимости **от категории доступа** к ней подразделяется на **общедоступную информацию**, а также на информацию, доступ к которой ограничен федеральными законами (**информация ограниченного доступа**).

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. «Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации».

Кроме того, по закону, информация в зависимости **от порядка предоставления или распространения** подразделяется на информацию:

1) свободно распространяемую;

2) предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) подлежащую предоставлению или распространению в соответствии с федеральными законами;

4) ограниченную или запрещенную для распространения в Российской Федерации.

Закон РФ «О средствах массовой информации», принятый в 1991 году, определяет понятие «**массовая информация»,** как «предназначенные для неограниченного круга лиц печатные, аудиовизуальные и иные сообщения и материалы».

Хотя в новом законе ФЗ № 149-ФЗ нет определения «защищаемая информация», в нем есть определение «защиты информации». (Защиту информации иногда путают с информационной безопасностью.)

**«Защита информации** представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации».

Это определение, конечно, требует комментария и сравнения с другими определениями из других документов.

В п.1 есть перечисление неправомерных действий, хотя неполное, но информативное.

П. 2 касается только конфиденциальности, хотя можно потребовать и целостность и доступность и другое.

П. 3 некоторым образом все же касается обеспечения доступности информации.

Забегая вперед можно сказать, что это определение в своих пунктах фактически перефразирует требования по целостности, конфиденциальности и доступности информации, о которых будет сказано далее.

Для сравнения приведем ряд других определений, собранных в словаре Парфенова В.И., который вышел в 2003 году.

**Защита информации -**

1) деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [ГОСТ Р 50922-96 ЗИ. Основные термины и определения];

2) все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей. Она включает криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера [Указ Президента РФ №1268 от 26 авг 1996];

3) комплекс мероприятий проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации [Положение о госуд. Лицензировании в обл. ЗИ от 27 апр. 1994];

4) организационные, программные и технические методы и средства, направленные на удовлетворение ограничений, установленных для типов данных или экземпляров типов данных в системе обработки данных [Толк. Словарь по информатике, 1991];

Далее отдельно будет рассмотрено понятие **«количества информации»,** которое изучалось и оценивалось многими исследователями (Шеннон, Винера, Бриллюэн и др.). Например, К.Шеннон определял количество информации в сообщении, как «меру неопределенности, которую оно устраняет для получателя». Отсюда путь через неопределенность, случайные величины, энтропию.

К. Шеннон предложил единицу измерения информации — бит. Количество информации описывается формулой вида:

H = - Σi=1n pi log pi

где р\_i — вероятность появления i-го сигнала; n — количество возможных сигналов. (В обыденном понимании — чем неожиданнее новость, тем больше ее информативность.)

[Колмогоров А.Н.](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D0%BC%D0%BE%D0%B3%D0%BE%D1%80%D0%BE%D0%B2%2C_%D0%90%D0%BD%D0%B4%D1%80%D0%B5%D0%B9_%D0%9D%D0%B8%D0%BA%D0%BE%D0%BB%D0%B0%D0%B5%D0%B2%D0%B8%D1%87) в работе «Три подхода к определению понятия «Количество информации» сформулировал три способа определения количества информации: комбинаторный, вероятностный и алгоритмический. [Новое в жизни, науке, технике. Сер. "Математика, кибернетика", N1, 1991, С.24-29 или "Проблемы передачи информации", N1, 1965, С.1-7].

Однако математическая теория информации не охватывает всего богатства содержания информации, поскольку она, прежде всего, абстрагируется от содержательной (семантической) стороны сообщения. С точки зрения этой теории, «совокупность 100 букв, выбранных случайным образом, фраза в 100 слов из газеты, пьесы Шекспира или теорема Эйнштейна имеют в точности одинаковое количество информации». Тем не менее глубокие теоретические и практические результаты были получены, например, в области секретной связи.

Актуальными являются сегодня и понятия «**информационная инфраструктура**», «**критические сегменты информационной инфраструктуры**» и др.

Предметом защиты является не только информация. В настоящее время в связи с рассматриваемой областью говорят об **активах (ресурсах),** а информация рассматривается как их часть.

В ряде документов **активы или ресурсы** (assets) – это «все, что имеет ценность для организации» [См. например, ISO/IEC 13335-1:2004]. Стандарт банка России уточняет это определение. В частности, согласно стандарту СТО БР ИББС 1.0-2006, активы организации банковской системы Российской Федерации: “все, что имеет ценность для организации банковской системы Российской Федерации и **находится в ее распоряжении**”.

К активам организации (Банка) могут относиться:

- банковские ресурсы (финансовые, людские, вычислительные, телекоммуникационные и пр.);

- информационные активы на следующих фазах их **жизненного цикла**: генерация (создание), обработка, хранение, передача, уничтожение;

- банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы, процессы жизненного цикла автоматизированных банковских систем и др.);

- банковские продукты и услуги.

В свою очередь информационные активы делятся на следующие типы:

финансово - аналитическая информация;

служебная информация;

управляющая информация общего и специального назначения;

справочная информация;

информация операционной и телекоммуникационной среды

платежная информация.

В качестве одного из важнейших активов также рассматривается **репутация организации**. В последнее время часто оценивается и так называемый **брэнд** организации или торговой марки.

Все активы организации должны быть идентифицированы и классифицированы удобным и приемлемым для нее образом. Примеры рекомендаций для этого даны в проекте рекомендаций Банка России **РС БР ИББС- 2.3-2008**.

Среди объектов защиты особую роль играют приводимые ниже объекты, определение которым мы приводим в данном разделе.

Помимо понятия «информационная система» важно и используются понятия «автоматизированная система», «автоматизированная информационная система» и, в частности, «автоматизированная банковская система».

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [ГОСТ 34.003-90]. В зависимости от вида деятельности выделяют виды автоматизированных систем:

АСУ – автоматизированная система управления,

САПР – система автоматизации проектирования, … .

Обращает внимание то, что персонал учитывается при определении автоматизированной системы, в отличие от определения «информационной системы» и следующего определения.

**Автоматизированная информационная система** – комплекс программных и технических средств, предназначенных для сбора, хранения, поиска и выдачи информации по запросам [Толковый словарь по информатике, М.: Ф и Ст, 1991].

**Автоматизированная банковская система**: автоматизированная система, реализующая банковский технологический процесс или его часть.

Сразу определим, что такое банковский технологический процесс, упомянутый в определении.

**Банковский технологический процесс:** технологический процесс, содержащий операции по изменению и(или) определению состояния банковской информации, используемой при функционировании или необходимой для реализации банковских услуг. В зависимости от вида деятельности выделяют: **банковский информационный технологический процесс**, **банковский платежный технологический процесс** и др.

Чтобы определить, что такое «информационная безопасность», рассмотрим сначала само понятие «**безопасности**». Здесь тоже имеет место различие мнений и определений.

Вл. Даль определял, что «**безопасность** – есть отсутствие опасности, сохранность, надежность».

В толковом словаре русского языка Ожегова С.И. сказано, что « **безопасность** – состояние, в котором не угрожает опасность, есть защита от опасности».

Закон «О безопасности» 1992 года гласит, что «**безопасность** – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних **угроз**». Появилось новое понятие «угрозы», близкое к понятию «опасности», упоминавшихся у Даля и Ожегова.

Приведем некоторые определения понятия «угрозы» по времени их появления в документах.

1. **Угроза** - совокупность условий и факторов, создающих опасность жизненноважным интересам личности, общества и государства [ФЗ О безопасности 05.03.1992].

2. **Угроза** - потенциальный источник возникновения **ущерба** [ГОСТ Р 51898-2002 п.3.5].

3. **Угроза** - потенциальная причина **инцидента**, который может нанести **ущерб** системе или организации. [ISO/IEC 13335-1:2004]

Как видно появляются новые понятия «инцидента» и «ущерба».

Сначала рассмотрим понятие «инцидент», но не просто, а именно «инцидент информационной безопасности».

**Инцидент информационной безопасности (information security incident)[ ГОСТ ИСО/МЭК 13335-1]:** Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

В качестве некоторых примеров инцидентов в ГОСТе указаны:

- утрата услуг, оборудования или устройств;

- системные сбои или перегрузки;

- ошибки пользователей;

- несоблюдение политик или рекомендаций;

- нарушение физических мер защиты;

- неконтролируемые изменения систем;

- сбои программного обеспечения и отказы технических средств;

- нарушение правил доступа.

Более сложно понятие «инцидента» определено в стандарте [ ISO/IEC 18044: 2004], через «событие ИБ».

**Инцидент** - событие, являющееся следствием одного или нескольких нежелательных или неожиданных **событий (информационной безопасности)**, имеющих значительную вероятность компрометации бизнес - операции и создания угрозы.[ ISO/IEC 18044: 2004].

**Событием (информационной безопасности)** является идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение **политики информационной безопасности** или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.[ ISO/IEC 18044: 2004].

В стандарте Банка России понятие «инцидента» распространено на организацию банковской системы РФ.

**Инцидент информационной безопасности организации банковской системы Российской Федерации**: событие, вызывающее действительное, предпринимаемое или вероятное нарушение информационной безопасности организации банковской системы Российской Федерации.

Нарушение может вызываться либо ошибкой людей, либо неправильным функционированием технических средств, либо природными факторами (например, пожар или наводнение), либо преднамеренными злоумышленными действиями, приводящими к нарушению конфиденциальности, целостности, доступности, учетности или неотказуемости.

С инцидентом связано следующее понятие.

**Воздействие (impact):** Результат нежелательного инцидента информационной безопасности.

Говоря об угрозах часто используется понятие «**модели угроз**», которая, согласно СТО БР ИББС 1.0-2006, «включает описание **источников угроз**, **уязвимостей**, используемых угрозами, **методов и объектов нападений**, пригодных для реализации угрозы, **типов возможной потери**, **масштабов потенциального ущерба**».

Разберем понятие «модели угроз» по составляющим.

**Источник угроз** - субъект, материальный объект или физическое явление, создающее угрозу безопасности информации.

Для источников угроз – людей – разрабатывается **модель нарушителя.** В модели нарушителя конкретизируются субъекты, их средства, знания и опыт, с помощью которых они могут реализовать угрозы и нанести ущерб объектам, а также мотивации их действий.

Частным видом нарушителя является злоумышленник. **Злоумышленник** – основной субъект угроз, источник противоборства с собственником в борьбе за активы и доходы.

**Уязвимость** - недостатки или слабые места активов, которые могут быть использованы угрозой .[СТО БР ИББС-1.0 -2006]. Наличие уязвимости без присутствия угрозы не причиняет ущерба, но все уязвимости должны контролироваться на предмет изменения ситуации. Также и угрозы, не имеющие соответствующих уязвимостей, не приводят к ущербу, но должны учитываться.

**Ущерб** – физическое повреждение или другой вред здоровью людей, имуществу (активам) или окружающей среде. Количественная величина ущерба не всегда поддается оценке. В этих случаях для оценки ущерба может использоваться качественное описание.

Отечественный ГОСТ Р 51898 – 2002 определяет, что «**безопасность** – отсутствие недопустимого **риска**». То есть определяет через другое понятие «риска», которое более емко, чем просто понятие «опасности». К тому же упоминается не просто риск, а недопустимый риск. На этом понятие остановимся подробнее.

**Риск** – сочетание вероятности нанесения ущерба и тяжести этого ущерба [ГОСТ Р 51898-2002 Аспекты безопасности].

В этом [ГОСТ Р 51898-2002 ] также сказано, что термин «риск» обычно используют только тогда, когда существует возможность негативных последствий, а в некоторых ситуациях риск обусловлен возможностью отклонения от ожидаемого результата или события.

**Риск** – сочетание вероятности события и его последствий.[Guide 73: 2002 Risk Management – Vocabulary – Guidelines for use in standards].

**Риск** - неопределенность, предполагающая возможность потерь (ущерба) [СТО БР ИББС 0.1-2006].

Следует пояснить суть употребления слова «**вероятность**» в этих определениях. Об этом подчеркивается, например, и в известном австралийском стандарте AS/NZS 4360:2004 “Risk management”. Вероятность здесь не математическое понятие и число между 0 и 1, а возможность или частота события. Часто вероятность оценивается качественно, например, в терминах «низкая», «средняя», «высокая».

На практике можно встретить следующие виды рисков:

- стратегический риск,

- юридический риск,

- операционный риск,

- репутационный риск,

- рыночный риск,

- кредитный риск,

- инвестиционный риск,

- политический риск,

- проектный риск,

- ИТ - риск,

- риск информационной безопасности,

и другие.

Не вдаваясь здесь в подробное описание всех перечисленных рисков, приведем определение некоторых из важнейших.

**Информационный риск (ИТ - риск)** — это опасность возникновения убытков или ущерба в результате применения информационных технологий.

Иными словами, IT-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи (М. Мур). С информационным риском наиболее связаны операционный риск и риск информационной безопасности.

**Операционный риск** - риск убытков, связанных с неадекватными либо неудачными внутренними процессами, действиями персонала или систем, а также в связи с внешними событиями. Операционный риск включает в себя юридический риск, но не включает стратегический и репутационный риск.

Это определение из рекомендаций Базель-2 в переводе ЦБ РФ. В подлиннике оно такое.

**«Operational risk** is defined as: .the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk. However, strategic and reputational risk is not included in this definition for the purpose of a minimum regulatory operational risk capital charge».

На мой взгляд, лучше следующий перевод.

**Операционный риск** определяется как риск прямых или косвенных потерь от неадекватных или имеющих недостатки внутренних процессов, людей и систем или от внешних событий.

Суть в том, что персонал – это только часть людей. Внешние злоумышленники сюда не входят.

Это один из примеров сложности перевода англоязычных терминов.

Определение **риска информационной безопасности** будет далее.

Завершая тему «риска» необходимо дать определение из [ГОСТ Р ИСО/МЭК 17799].

**Менеджмент риска (risk management):** Скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание - Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникация риска.[ISO/IEC Guide 73:2002]

Или

**Менеджмент риска (risk management):** Полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий.

Это одно из определений, взятое из [ГОСТ Р ИСО/МЭК 13335-1] . Далее вопросу менеджмента или управления рисками будет уделено внимание в отдельном курсе. Там будет нужна целая терминосистема по рискам.

**Остаточный риск (residual risk):** Риск, остающийся после его обработки.

**Анализ риска (risk analysis):** систематический процесс определения величины риска.

**Оценка риска (risk assessment):** процесс, объединяющий идентификацию риска, анализ риска и оценивание риска.

**(Оценка риска (risk assessment):** общий процесс анализа риска и оценка степени риска. Это определение из [ISO/IEC Guide 73:2002] используется в ГОСТ Р ИСО/МЭК 17799-2005. Там же используется понятие

**Оценивание риска (risk evaluation):** Процесс сравнения оцененного риска с данными критериями риска с целью определения значимости риска.[ISO/IEC Guide 73:2002]. Это еще один из примеров трудности перевода.

**Обработка риска (risk treatment):** Процесс выбора и осуществления мер по модификации риска. ( Аналогично как в [ISO/IEC Guide 73:2002] и [ГОСТ Р ИСО/МЭК 17799-2005.]) Обработка риска включает: предотвращение, перенос, снижение и принятие риска. После обработки рисков могут оставаться **остаточные риски**.

Другие элементы терминосистемы по рискам будут рассмотрены отдельно.

**Защитная мера (или мера защиты, контрмера, мера контроля)** - мера, используемая для уменьшения риска [ГОСТ Р 51898-2002, **ISO/IEC Guide 51**].

Или, по другому, **защитная мера (safeguard):** сложившаяся практика, процедура или механизм обработки риска. В контексте безопасности информационно-телекоммуникационных технологий термин «защитная мера» может считаться синонимом термина «контроль» [ГОСТ Р ИСО/МЭК 13335-1]

**Базовые защитные меры (baseline controls):** минимальный набор защитных мер, установленный для системы или организации.[ГОСТ Р ИСО/МЭК 13335-1]. Они соответствуют **базовому уровню безопасности** (Baseline Security) – обязательный минимальный уровень защищенности для информационных систем. В ряде стран существуют требования к системе защитных мер, соответствующих этому уровню (CCTA Baseline security survey- Великобритания, BSI IT-Grundschutz – Германия, ISACA, …).

Контрмеры базового уровня служат для защиты от стандартного набора наиболее распространенных угроз (вирусы, сбои оборудования, не санкционируемый доступ и т.д.).

В целом средства контроля могут обеспечивать один или несколько из следующих **видов защиты**: предупреждение, сдерживание, обнаружение, снижение, восстановление, исправление, мониторинг и информированность.

Удобно далее говорить **о системе обеспечения безопасности**.

Она включает силы и средства обеспечения безопасности, которые действуют и используются на основе разработанных заранее и закрепленных некоторым формальным образом принципов и правил (в виде нормативно-правовых актов, ведомственных инструкций, положений и т.п.).

Можно говорить, что **сущность функционирования системы безопасности** заключается в выявлении, прогнозировании, предотвращении, нейтрализации, пресечении, локализации, устранении, отражении и уничтожении угроз защищаемому объекту, а также формировании условий, благоприятствующих деятельности данного объекта, достижения им своих целей, защиты его интересов.

Система обеспечения безопасности того или иного объекта решает следующие задачи:

1. Своевременное выявление и прогнозирование внешних и внутренних угроз.

2. Осуществление комплекса оперативных и долговременных мер по предупреждению и нейтрализации внутренних и внешних угроз.

3. Создание и поддержание в готовности сил и средств для обеспечения безопасности.

4. Управление силами и средствами обеспечения безопасности в нормальных (повседневных) условиях и при возникновении чрезвычайных ситуаций.

5. Осуществление системы мер по нормальному функционированию объектов безопасности после возникновения чрезвычайных ситуаций.

6. Участие в мероприятиях по обеспечению безопасности за пределами своего объекта в соответствии с договоренностями (соглашениями) внутри корпорации или объединения фирм (предприятий).

В последнее время все чаще в обиход входит понятие **система комплексной безопасности** [Тихонов, Райх, Информ безоп, 2006]. Под этим термином понимается совокупность организационных мероприятий и действий подразделений охраны и служб безопасности организаций и автоматизированных систем по защите информации, направленных на обеспечение установленного режима, порядка и правил поведения, предотвращение, обнаружение и ликвидацию угроз жизни, среде обитания, имуществу и информации, а также поддержание работоспособности технических средств и систем на охраняемом объекте с целью ограничения или предотвращения действий нарушителя для осуществления опасных несанкционированных операций на объекте, приводящих к частичному или полному нарушению функционирования данного объекта.

Фактически в этом определении просто расширен список угроз безопасности.

Говоря о безопасности, уместно вспомнить ФЗ «О техническом регулировании» 2002 года. В нем определена «**безопасность продукции, процессов производства, эксплуатации**, **хранения, перевозки, реализации и утилизации»,** как «состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государству или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений».

Перейдем от понятия «безопасность» к понятию «информационная безопасность».

Понятие «**информационная безопасность**» была нормативно закреплена в качестве самостоятельной составляющей понятия безопасности в ФЗ «О безопасности» в 1992 году.

Далее в 1996 году в ФЗ «Об участии в международном информационном обмене сказано, что «**информационная безопасность** – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства». Здесь «**информационная среда** - сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации».

В Доктрине информационной безопасности РФ от 2000 года, это определение приспособлено и уточнено для России. Именно под «**информационной безопасностью Российской Федерации**» понимается – состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Вообще, обычно понятие «информационной безопасности» (ИБ) надо уточнять – информационная безопасность чего?

В словаре Парфенова В.И. можно встретить определения:

- ИБ автоматизированных систем (АС), ИБ государства, ИБ личности, ИБ мирового сообщества, ИБ новых информационных технологий, ИБ общества, ИБ РФ. Этот список можно продолжать. Приведем здесь только одно из определений.

**Информационная безопасность автоматизированных систем** (АС)– область науки и техники, охватывающая совокупность программно-аппаратных, криптографических, технических и организационно-правовых методов и средств обеспечения безопасности информации в автоматизированных системах при ее обработке, хранении и передаче с использованием современных информационных технологий (Погорелов Б.А., Мацкевич И.Б. 1977).

Здесь вызывает возражение только упоминание «современных» технологий. Обращает на себя внимание другая классификация мер защиты, выделение криптографических методов и средств.

Многие вариации определений информационной безопасности были основаны на определении из британского стандарта BS 7799, вышедшего в 1995 году, где сказано, что **информационная безопасность** – защищенность ресурсов информационной системы от факторов, представляющих угрозу для конфиденциальности, целостности и доступности.

**Доступность (availability):** Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта. [ИСО/МЭК 7498-2]

Или проще, **Доступность** – это возможность за приемлемое время получить требуемую информационную услугу.

**Целостность (integrity):** Свойство сохранения правильности и полноты активов. [ ГОСТ Р ИСО/МЭК 13335-1]

Или **Целостность** – это актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

**Конфиденциальность (confidentiality):** Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса. [ИСО/МЭК 7498-2].

Есть и другие аспекты безопасности. К тому же приведенные аспекты конфиденциальности, целостности и доступности в разных системах имеют разный вес.

В ГОСТ Р ИСО/МЭК 13335-1:2005 это перечисление в определении больше.

**Информационная безопасность (information security):** все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Приведем те, которые еще не определены ранее.

**Неотказуемость (non-repudiation):** способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты. [ИСО/МЭК 13888-1, ИСО/МЭК 7498-2, ГОСТ Р 13335-1]

**Подотчетность (учетность, отслеживаемость) (accountability):**свойство, обеспечивающее однозначное прослеживание действий любого логического объекта. [ИСО/МЭК 7498-2]

Иногда переводится как **«учетность»,** например в стандарте Банка России.

**Аутентичность (authenticity):** Свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Примечание — Аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

**Достоверность (reliability):** Свойство соответствия предусмотренному поведению и результатам.

Исторически к конфиденциальности было больше внимания. С этим понятием связано понятие **«тайна»**, которая имеет множество производных: г[осударственная тайна](http://cyber-crimes.ru/laws/protected/?ID=State), [коммерческая тайна](http://cyber-crimes.ru/laws/protected/?ID=Commercial), [адвокатская тайна](http://cyber-crimes.ru/laws/protected/?ID=Attorney), [банковская тайна](http://cyber-crimes.ru/laws/protected/?ID=Bank), [врачебная тайна](http://cyber-crimes.ru/laws/protected/?ID=Medical), налоговая тайна, нотариальная тайна, [персональные данные, личная и семейная тайна](http://cyber-crimes.ru/laws/protected/?ID=Personal), [служебная тайна](http://cyber-crimes.ru/laws/protected/?ID=Commercial), тайна голосования, [тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений](http://cyber-crimes.ru/laws/protected/?ID=Correspondence), [тайна следствия и судопроизводства](http://cyber-crimes.ru/laws/protected/?ID=Investigation), т[айна совещания судей](http://cyber-crimes.ru/laws/protected/?ID=Judge), тайна страхования, тайна усыновления (удочерения), аудиторская тайна и др. (всего около 40 ). Приведем некоторые из них, которым посвящены отдельные законы Российской Федерации в силу их важности.

**Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.[Закон РФ «О государственной тайне»].

В этом определении не уточняется, какие свойства сведений защищаются. Да и вообще, определение «тайны» через «сведения» не очень хорошо. Лучше следующее определение.

**Коммерческая тайна** – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.[ФЗ РФ « О коммерческой тайне», 2004]

Хотелось бы дать и собственное определение **информационной безопасности**, как «безопасности, связанной с информацией или с информационной сферой».

По аналогии с этим определением можно понять и определить, что такое:

**государственная безопасность,**

**экономическая безопасность,**

**энергетическая безопасность,**

**экологическая безопасность,**

**пожарная безопасность,**

**транспортная безопасность,**

**банковская безопасность,**

и другие.

Понятие информационной безопасности, включая в себя **компьютерную безопасность** в качестве неотъемлемой составной части. Кроме того, по своему содержанию информационная безопасность включает:

- компьютерную безопасность;

- безопасность информационных систем и процессов;

- безопасность среды для реализации информационных процессов.

Приведем здесь определение компьютерной безопасности из словаря Парфенова В.И. или из книги [Теоретические основы информатики и информационная безопасность. М.: Радио и связь, 2000.-468 с.]

**Компьютерная безопасность -** свойство компьютерной информации, ЭВМ, системы ЭВМ, сети ЭВМ, при котором с требуемой вероятностью обеспечивается защита компьютерной информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, копирования, блокирования, а также защита ЭВМ, системы ЭВМ, сети ЭВМ от неправомочного доступа, создания, использования и распространения вредоносных программ, нарушения правил эксплуатации, несанкционированной модификации программ и т.п..

Помимо **системы обеспечения (информационной)безопасности** важна **система менеджмента информационной безопасности**.

В частности для организаций банковской системы есть определение.

**Система менеджмента (управления – в некоторых документах) информационной безопасности организации банковской системы Российской Федерации; СМИБ (СУИБ) –** эточасть общей системы менеджмента организации банковской системы Российской Федерации, основывающаяся на подходе бизнес-риска, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности организации банковской системы Российской Федерации [ISO/IEC IS 27001].

Система менеджмента включает структуру, политики, деятельности по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

Важнейшими исходными данными для эффективной деятельности служб ИБ являются информационные модели основной деятельности организации (описания бизнес-процессов, реализуемых технологий и т.п.). Данные модели определяют контекст и акценты внимания деятельности служб ИБ, так как они позволяют понять, где в структуре деятельности организации в части информатики имеются уязвимости для потенциальных злоумышленников и какие защитные меры могут потребоваться и какие из них могут быть наиболее эффективными.

Результатами (выходами) деятельности и процессов по обеспечению ИБ организации являются:

- документы (отчеты, предложения, внутренние нормативные документы);

- механизмы (средства) обеспечения ИБ и решения по их реконфигурации (совершенствованию);

- сигнал опасности для основной деятельности (бизнеса) организации.

Механизмы обеспечения ИБ, являющиеся результатом деятельности и процессов по ее обеспечению в организации, выступающие в качестве ресурсного обеспечения для основной деятельности организации, эксплуатируются службами ИБ, а в отдельных случаях и основными функциональными подразделениями организации. Информация контроля результатов применения и функционирования механизмов (защитных мер) поступает для анализа в службу информационной организации.

Остановимся подробнее на важном понятии «**политика безопасности**». Приведем несколько определений.

**Политика безопасности организации –** одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Далее появились разновидности этого определения. Например, такое.

**Политика безопасности информационно-телекоммуникационных технологий** (политика безопасности ИТТ) (ICТ security policy): правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию. [ГОСТ Р 13335-1].

Нас будет в основном интересовать «политика информационной безопасности». Согласно [ГОСТ Р ИСО/МЭК 17799-2005]

**Политика информационной безопасности** должна быть утверждена высшим руководством, издана и доведена до сведения всех сотрудников и соответствующих внешних сторон.

Документ о политике информационной безопасности должен устанавливать ответственность руководства и излагать подход организации к управлению информационной безопасностью. Политика должна содержать следующие положения:

а) определение информационной безопасности, ее общих целей и сферы действия, а также упоминание значения безопасности как инструмента, обеспечивающего возможность совместного использования информации (см. Введение);

б) изложение намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;

в) основание для установки целей контроля и мер контроля, включая структуру оценки риска и менеджмент риска;

г) краткое изложение наиболее существенных для организации политик безопасности, принципов, стандартов и требований, включающее:

1) соответствие законодательным, регулятивным требованиям и договорным обязательствам;

2) требования в отношении обучения и осведомлённости в вопросах безопасности;

3) управление непрерывностью бизнеса;

4) ответственность за нарушения политики информационной безопасности;

д) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

е) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Такая политика информационной безопасности должна быть доведена до сведения пользователей в рамках всей организации в уместной, доступной и понятной форме.

Политика информационной безопасности может быть частью документа общей политики. Если политика информационной безопасности распространяется вне организации, то нужно обратить внимание на неразглашение секретной информации. Дополнительную информацию можно найти в ISO/IEC 13335-1:2004.

Политика информационной безопасности должна пересматриваться через запланированные промежутки времени или в случае появления существенных изменений в целях обеспечения её непрерывной стабильности, адекватности и эффективности

Политика информационной безопасности должна иметь владельца, который утвердил административную ответственность за развитие, пересмотр и оценку политики безопасности. Пересмотр должен включать возможности оценки для улучшения политики информационной безопасности организации и подход к управлению информационной безопасностью в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.

В стандарте Банка России понятие политики ИБ банковской системы приводится похожее на предыдущие определение.

**Политика информационной безопасности организации банковской системы Российской Федерации**: одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется организация банковской системы Российской Федерации в своей деятельности.

Завершает раздел **исходная концептуальная схема (парадигма) обеспечения информационной безопасности**, которая обсуждается в работе [Курило и др]. **Суть парадигмы ИБ** — противоборство собственника и злоумышленника за права на информационные активы в целях последующего извлечения дохода.

На самом деле, цели злоумышленника могут быть и другие. Поэтому это понятие трактуется и конкретизируется в стандарте Банка России следующим образом.

В основе **исходной концептуальной схемы информационной безопасности организаций БС РФ** лежит противоборство собственника и злоумышленника за контроль над информационными активами. В случае если злоумышленник устанавливает контроль над информационными активами, как самой организации БС РФ, так и клиентам, которые доверили ей свои собственные активы, может быть нанесен ущерб.

**Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.**

В Концепции национальной безопасности РФ, утвержденной Указом Президента РФ от 17.12.1997 г. № 1300 (в редакции Указа Президента РФ от 10.01.2000 г. №24) [БЛ], дается следующее определение национальной безопасности.

Под **национальной безопасностью РФ** понимается безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в РФ.

**Национальные интересы России** - это совокупность сбалансированных интересов личности, общества и государства в различных сферах жизнедеятельности: экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других.

В теории национальной безопасности используется понятие **«жизненно важные интересы».**

**Жизненно важные интересы** - это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства [БЛ]. Как правило понятия «национальные интересы» и «жизненно важные интересы» являются идентичными.

Национальные интересы носят долгосрочный характер. В области внутренней и внешней политики государства этими интересами определяются:

• основные цели этой политики;

• стратегические и текущие задачи.

Национальные интересы обеспечиваются **институтами государственной власти**, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ **общественными организациями**.

Интересы личности состоят в реализации конституционных прав и свобод [БЛ], в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина.

Интересы общества состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

Национальные интересы России в **информационной сфере** заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных теле- коммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Важнейшими составляющими национальных интересов России являются защита личности, общества и государства от терроризма, в том числе международного, а также от чрезвычайных ситуаций природного и техногенного характера и их последствий, а в военное время - от опасностей, возникающих при ведении военных действий или вследствие этих действий.

Достижению национальных интересов препятствуют те или иные уязвимости и угрозы.

**Уязвимостями** для национальной безопасности страны являются - состояние отечественной экономики, несовершенство системы организации государственной власти и гражданского общества, социально-политическая поляризация российского общества, наличие организованной преступности и терроризма, обострение межнациональных и осложнение международных отношений и другие.

Усиливаются угрозы национальной безопасности РФ в информационной сфере. Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Обеспечение национальной безопасности РФ во многом определяется состоянием информационной безопасности.

Важнейшими задачами обеспечения информационной безопасности РФ являются:

• реализация конституционных прав и свобод граждан РФ в сфере информационной деятельности;

• совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

• противодействие угрозе развязывания противоборства в информационной сфере.

Основу системы обеспечения национальной безопасности РФ составляют органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера, направленные на обеспечение безопасности личности, общества и государства.

Полномочия органов и сил обеспечения национальной безопасности РФ, их состав, принципы и порядок действий определяются соответствующими законодательными актами РФ.

Условно можно выделить следующие **составляющие национальной безопасности**: экономическую, внутриполитическую, социальную, духовную, международную, информационную, военную, пограничную, экологическую.

Содержание каждой из перечисленных составляющих отражено в соответствующих **нормативных правовых актах**.

**Информатизация** является характерной чертой жизни современного общества. Новые информационные технологии активно внедряются во все сферы народного хозяйства. Компьютеры управляют космическими кораблями и самолетами, контролируют работу атомных электростанций, распределяют электроэнергию и обслуживают банковские системы. Компьютеры являются основой множества автоматизированных систем обработки информации (АСОИ), осуществляющих хранение и обработку информации, предоставление ее потребителям, реализуя тем самым современные информационные технологии.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, от которых порой зависит благополучие, а иногда и жизнь многих людей.

Актуальность и важность проблемы обеспечения безопасности информационных технологий обусловлены такими причинами, как:

• резкое увеличение вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации;

• резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;

• сосредоточение в единых базах данных информации различного назначения и различной принадлежности;

• высокие темпы роста парка персональных компьютеров, находящихся в эксплуатации в самых разных сферах деятельности;

• резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;

• бурное развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности;

• повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные;

• развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. **Информационная сфера** представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений [Доктрина ИБ РФ].

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать [Доктрина ИБ РФ].

Напомним, что под **информационной безопасностью РФ** понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [Доктрина ИБ РФ].

Доктрина информационной безопасности РФ дает **две классификации национальных интересов в информационной сфере**:

• первую классификацию можно назвать классификацией по принадлежности интересов;

• вторую классификацию можно назвать классификацией по важности интересов.

В соответствии с первой классификацией национальные интересы -это совокупность интересов личности, интересов общества и интересов государства.

**Содержание интересов личности, общества и государства в информационной сфере**

**Интересы личности:**

• Реализация конституционных прав на доступ к информации.

• Использование информации в интересах осуществления не запрещенной законом деятельности.

• Физическое, духовное и интеллектуальное развитие.

• Защита информации, обеспечивающей личную безопасность.

**Интересы общества**

• Обеспечение интересов личности в информационной сфере.

• Упрочение демократии, создание правового, социального государства.

• Достижение и поддержание общественного согласия.

• Духовное обновление России.

**Интересы государства**

• Гармоничное развитие российской информационной инфраструктуры.

• Реализация конституционных прав человека и гражданина в области получения информации и пользования ею.

• Незыблемость конституционного строя, суверенитета и территориальной целостности России.

• Политическая, экономическая и социальная стабильность.

• Безусловное обеспечение законности и поддержание правопорядка.

• Развитие равноправного и взаимовыгодного международного сотрудничества.

**Угрозы и источники угроз в информационной сфере Российской Федерации**

По своей общей направленности угрозы информационной безопасности РФ подразделяются на следующие виды [Доктрина ИБ РФ]:

1.• угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

2.• угрозы информационному обеспечению государственной политики РФ;

3.• угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

4.• угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

**Источники угроз** информационной безопасности РФ подразделяются на внешние и внутренние.

**Внешними источниками** являются:

• деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;

• стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

• обострение международной конкуренции за обладание информационными технологиями и ресурсами;

• деятельность международных террористических организаций;

• увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

• деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

• разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

**Внутренними источниками** являются:

• критическое состояние отечественных отраслей промышленности;

• неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

• недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;

• недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

• неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

• недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;

• недостаточная экономическая мощь государства;

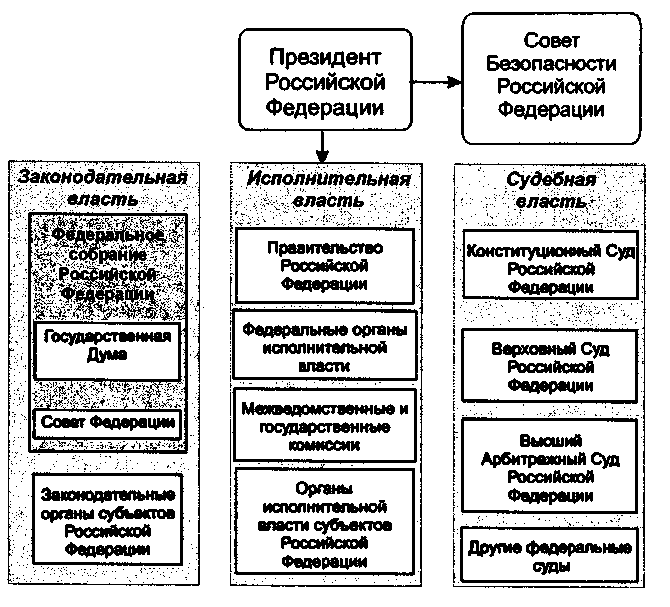
• снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

• недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

• отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Хотя в Доктрине и приведены эти внутренние источники, но фактически они являются не источниками, а уязвимостями. Все зависит от понимания этих понятий.

**Общая структура государственной системы обеспечения информационной безопасности Российской Федерации**



Рассмотрим **структуру государственной системы информационной безопасности** и основные функции ее составных частей.

Основным органом, координирующим действия государственных структур по вопросам защиты информации, является Межведомственная комиссия по защите государственной тайны, созданная Указом Президента РФ № 1108 от 8.11.1995 г. Она действует в рамках Государственной системы защиты информации от утечки по техническим каналам, положение о которой введено в действие постановлением Правительства РФ от 15.09.1993 г. №912-51. В этом постановлении определены структура, задачи и функции, а также организация работ по защите информации применительно к сведениям, составляющим государственную тайну. Основной задачей Государственной системы защиты информации является проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности страны.

Президент РФ, Совет безопасности, Государственная дума, Межведомственная комиссия по защите государственной тайны, ФСТЭК, ФСБ, СВР и др.

Общая организация и координация работ в стране по защите информации, обрабатываемой техническими средствами, осуществляется **Федеральная служба по техническому и экспортному контролю (ФСТЭК России).**

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по следующим вопросам в области обеспечения информационной безопасности:

1) обеспечению безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;

2) противодействию иностранным техническим разведкам на территории РФ;

3) обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращению ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории РФ;

4) защите информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

**Основными задачами** в области обеспечения информационной безопасности для ФСТЭК России являются:

1) реализация в пределах своей компетенции государственной политики в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;

2) осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

3) организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой;

4) осуществление самостоятельного нормативно-правового регулирования вопросов: обеспечения безопасности информации в ключевых системах информационной инфраструктуры; противодействия техническим разведкам; технической защиты информации; размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров РФ, иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ; координации деятельности органов государственной власти по подготовке развернутых перечней сведений, подлежащих засекречиванию, а также методического руководства этой деятельностью;

5) обеспечение в пределах своей компетенции безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

6) прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;

7) противодействие добыванию информации техническими средствами разведки, техническая защита информации;

8) осуществление координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ и организаций по государственному регулированию размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров РФ, иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ;

9) осуществление в пределах своей компетенции контроля деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

10) осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны.

ФСТЭК России в своей деятельности руководствуется Конституцией РФ, федеральными конституционными законами, федеральными законами, актами президента РФ и правительства РФ, международными договорами РФ, приказами и директивами министра обороны РФ в части, касающейся ФСТЭК России, положением о ФСТЭК России, а также другими нормативными правовыми актами РФ, касающимися деятельности ФСТЭК России.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов РФ, федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, органами местного самоуправления и организациями.

ФСТЭК России осуществляет свою деятельность во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, органами местного самоуправления и организациями.

Обеспечение информационной безопасности является одним из основных направлений деятельности органов **Федеральной службы безопасности (ФСБ) России**.

Обеспечение информационной безопасности осуществляется ими в пределах своих полномочий:

• при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;

• при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в РФ и ее учреждениях, находящихся за пределами РФ.

**Служба внешней разведки РФ** для осуществления своей деятельности может при собственных лицензировании и сертификации приобретать, разрабатывать (за исключением криптографических средств защиты), создавать, эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации от утечки по техническим каналам.

**Министерство обороны (Минобороны России)** организует деятельность по обеспечению информационной безопасности, защите государственной тайны в Вооруженных силах, а также в установленном порядке в пределах своей компетенции работы по сертификации средств защиты информации.

Другие органы государственного управления (министерства, ведомства) в пределах своей компетенции:

• определяют перечень охраняемых сведений;

• обеспечивают разработку и осуществление технически и экономически обоснованных мер по защите информации на подведомственных предприятиях;

• организуют и координируют проведение НИОКР в области защиты информации в соответствии с государственными (отраслевыми) программами;

• разрабатывают отраслевые документы по защите информации;

• контролируют выполнение на предприятиях отрасли установленных норм и требований по защите информации;

• создают отраслевые центры по защите информации и контролю эффективности принимаемых мер;

• организуют подготовку и повышение квалификации специалистов по защите информации.

Для осуществления указанных функций в составе органов государственного управления функционируют научно-технические подразделения (центры) защиты информации и контроля.

На предприятиях, выполняющих оборонные и иные секретные работы, функционируют научно-технические подразделения защиты информации и контроля, координирующие деятельность в этом направлении научных и производственных структурных подразделений предприятия, участвующие в разработке и реализации мер по защите информации, осуществляющие контроль эффективности этих мер.

Кроме того, в отраслях промышленности и в регионах страны создаются и функционируют лицензионные центры, осуществляющие организацию и контроль за лицензионной деятельностью в области оказания услуг по защите информации, органы по сертификации средств вычислительной техники и средств связи, испытательные центры по сертификации конкретных видов продукции по требованиям безопасности информации, органы по аттестации объектов информатики.

**Государственная система обеспечения информационной безопасности** создается для решения следующих проблем, требующих законодательной поддержки:

• защита персональных данных;

• борьба с компьютерной преступностью, в первую очередь в финансовой сфере;

• защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;

• защита государственных секретов;

• создание системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;

• обеспечение безопасности АСУ потенциально опасных производств;

• страхование информации и информационных систем;

• сертификация и лицензирование в области безопасности, контроль безопасности информационных систем;

• организация взаимодействия в сфере защиты данных со странами-членами СНГ и другими государствами.

Ключевыми проблемами также являются.

1. Формирование законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, нормативного закрепления ответственности должностных лиц и граждан по соблюдению требований информационной безопасности.

2. Разработка механизмов реализации прав граждан на информацию.

3. Формирование системы информационной безопасности, обеспечивающей реализацию государственной политики в этой области.

4. Совершенствование методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

5. Разработка критериев и методов оценки эффективности систем и средств информационной безопасности.

6. Исследование форм и способов цивилизованного воздействия государства на формирование общественного сознания.

7. Комплексное исследование деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

Огромную роль в информационной сфере в России в настоящее время также играют Мининформсвязи и ФАИТ. Большую работу для обеспечения информационной безопасности кредитно-финансовой сферы РФ проводит Центральный Банк.

**Государственная информационная политика обеспечения информационной безопасности России**

Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах [Доктрина ИБ РФ]:

• соблюдении Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ;

• открытости в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающей информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;

• правовом равенстве всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающемся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

• приоритетном развитии отечественных современных информационных и телекоммуникационных технологий, производстве технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Первоочередными **мероприятиями по реализации государственной политики** **обеспечения информационной безопасности РФ** являются [Доктрина]:

• разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности РФ;

• разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;

• принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов РФ, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов РФ, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;

• развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ;

• гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

**Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.**

Информация в жизни современного общества играет значительную роль. Современные информационные технологии проникли практически во все сферы общественных отношений. Это привело к необходимости создания правовых норм, регулирующих область информационных отношений. Такие нормы необходимы в силу того, что информация обладает рядом специфических свойств, которые принципиально отличают ее от других объектов права. Украсть информацию можно, не проникая в помещение, в котором она хранится, и, к тому же, информация после похищения, как правило, остается в распоряжении владельца в неизменном виде.

**Правовое обеспечение информационной безопасности** заключается в исполнении существующих или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц, руководителей, пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной им информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к техническим средствам и информации. Целью законодательных мер по защите информации являются предупреждение и сдерживание потенциальных нарушителей.

Для уяснения правовой сущности различных документов, с помощью которых осуществляется регулирование отношений, связанных с обеспечением информационной безопасности, рассмотрим общеправовые понятия, прежде всего **понятие нормативности**, производными от которого являются понятия **правовой нормы**, **нормативного правового акта**, **нормативного документа**.

Всякий акт (документ), принятый уполномоченным законом органом или лицом в пределах своей компетенции, является правовым, поскольку он регулирует соответствующие отношения. Правовые акты могут быть обязательными для неопределенного круга лиц, иметь персональный или рекомендательный характер. Акты обязательные именуются **нормативными правовыми актами**, все другие **ненормативными правовыми актами**. Географические границы действия нормативных правовых актов определяются статусом принимающего их органа или должностного лица (федеральный, субъекта Российской Федерации, муниципальный). Нормативные правовые акты, принимаемые организациями, именуются **локальными**.

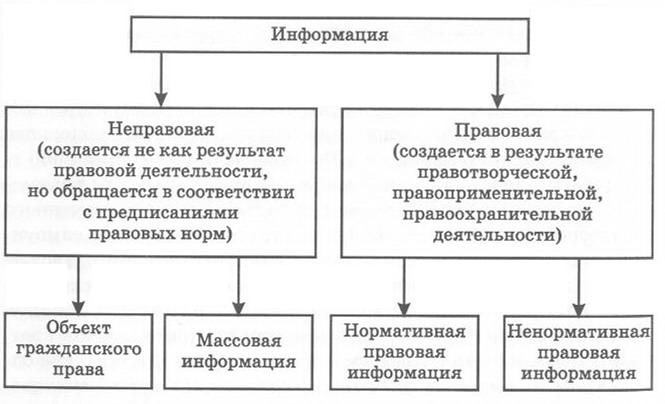
В законодательстве отсутствует определение понятия нормативного правового акта. Основные признаки нормативного правового акта даются в теории права, документах органов власти. В одном из постановлений Государственной Думы Федерального Собрания Российской Федерации за 1996 г. **нормативный правовой акт** определен как письменный официальный документ, принятый (изданный) в определенной форме правотворческим органом в пределах его компетенции и направленный на установление, изменение или отмену правовых норм. Под **правовой нормой** понимается общеобязательное правило поведения, установленное уполномоченным государственным органом и предназначенное для неоднократного применения.

В отличие от нормативного правового акта акт, устанавливающий, изменяющий или отменяющий права и обязанности конкретных лиц, именуется **правовым актом индивидуального характера**, или **ненормативным правовым актом**. К таким актам относятся, в частности, документы, используемые в правоприменительной деятельности.

Таким образом, нормативными правовым актами являются соответствующие законы Российской Федерации и субъектов Российской Федерации, указы Президента Российской Федерации, постановления Правительства Российской Федерации, акты федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, муниципальных органов, руководящих органов организаций.

Согласно Указу Президента Российской Федерации от 9 марта 2004 г № 314 «О системе и структуре федеральных органов исполнительной власти» право принимать нормативные акты имеют не все федеральные органы исполнительной власти, а только федеральные министерства. Но эти министерства в соответствии с Федеральным законом «О техническом регулировании» лишены такого права в сфере технического регулирования, где могут издавать только акты рекомендательного характера. Исключение из данного правила установлено в ст. 5 данного Закона в отношении специальной продукции, работ и услуг.

С учетом сказанного информацию в правовой системе по ее роли можно разделить на правовую и неправовую, как показано на рис. .



**Рис.**  Классификация информации по ее роли в правовой системе

Нормативная правовая информация создается в порядке пра­вотворческой деятельности и содержится в нормативных право­вых актах. Классификация такой информации по уровню при­нятия актов или по видам актов приведена на рис.

****

**Рис.** Классификация нормативной правовой информации по видам актов

Ненормативная правовая информация создается, как правило, в порядке правоприменительной и правоохранительной деятельности. С помощью такой информации реализуются предписания правовых норм. Эта информация создается в объекте управления и движется в контуре обратной связи системы правового управления.

На следующем рис. представлена обобщенная схема нормативно-правового и справочного обеспечения информационной безопасности (ИБ) информационных технологий (ИТ).

В соответствии с Конституцией России международные документы, подписанные от имени Российской Федерации, имеют приоритет над соответствующими документами федерального уровня. Документы, не подписанные от имени России, могут использоваться, если они не противоречат законодательству страны.

21

Рис. . Обобщенная схема нормативно-справочного обеспечения информационной безопасности (ИБ) информационных технологий

**Закон** – это нормативно- правовой акт, принимаемый высшим представительным органом государственной власти в особом законодательном порядке, обладающий высшей юридической силой и регулирующий наиболее важные общественные отношения с точки зрения интересов и потребностей населения страны.

**Подзаконные нормативно-правовые акты** – это правотворческие акты компетентных органов, которые основаны на законе и не противоречат ему. По своему содержанию подзаконные акты, как правило, являются актами различных органов исполнительной власти. По субъектам издания и кругу распространения они подразделяются на общие, местные, ведомственные и внутриорганизационные акты.

**Общие подзаконные акты** – это нормативно- правовые акты общей компетенции, действие которых распространяется на всех лиц в пределах территории страны. По своей юридической силе и значению – следуют за законами. Они исходят от президента страны или главы правительства.

**Указы президента** – в системе подзаконных актов обладают высшей юридической силой и издаются на основе и в развитии законов.

**Постановления правительства** – это подзаконные нормативные акты, принимаемые в контексте с указами президента и призванные урегулировать более мелкие вопросы государственного управления экономикой, образованием и т.д.

**Местные подзаконные акты –** это нормативно- правовые акты органов представительной власти на местах. Действие этих актов ограничено подвластной им территорией.

**Ведомственные нормативно- правовые акты (приказы инструкции)** – это нормативно- правовые акты общего действия, однако они распространяются лишь на ограниченную область общественных отношений (таможенные, банковские, транспортные и др.

**Внутриорганизационные подзаконные акты** – это такие нормативно- правовые акты, которые издаются различными организациями для регламентации своих внутренних вопросов и распространяются на членов этих организаций.

К числу **международных актов** относят: декларации; конвенции; рекомендации; соглашения; стандарты. Разработкой этих документов занимаются различные структурные подразделения международных организаций, такие как:

Организация объединенных наций;

Совет Европы (комитет министров);

Европейский комитет по проблемам преступности;

Комитет экспертов по преступности в киберпространстве (КЭ-ПК);

Международная электротехническая комиссия (МЭК/IEC);

Международная организация по стандартизации (ИСО/ISO);

Британский институт стандартов (BSI);

Американский институт AICPA;

и др.

В последующем Россия неоднократно выступала с инициативами в области международной информационной безопасности (резолюции Генеральной ассамблеи ООН A/RES/56/19 – ноябрь 2001 г., A/RES/57/53 – ноябрь 2002 г., A/RES/58/32 – декабрь 2003 г.). В соответствии с принятыми резолюциями с 2002 г. проходят Всемирные встречи на высшем уровне по вопросам информационного общества. Последняя из них состоялась 16‑18 ноября 2005 г. в Тунисе.

В 2004 г. была создана специальная Группа правительственных экспертов государств-членов ООН. Эта группа должна провести всестороннее исследование проблем международной информационной безопасностии подготовить свои рекомендации для их решения.

Среди всех международных нормативных актов в области информационной безопасности в нашей стране чаще всего применяются **организационно-технические документы**, в частности, **стандарты**. Большая часть из них принята в качестве национальных стандартов в сфере защиты информации.

**Отечественная федеральная и ведомственная нормативная базу по защите информации**  к настоящему времени включает более сотни нормативных документов, относящихся к вопросам информационной безопасности на государственном, региональном, местном, ведомственном уровнях. По своему назначению и содержанию их можно разделить на **три группы:**

1. Концептуальные документы, определяющие основу защиты информации в России.

2. Федеральные законы, определяющие систему защиты информации в России.

3. Вспомогательные нормативные акты в виде указов Президента РФ, постановлений Правительства РФ, межведомственных и ведомственных руководящих документов и стандартов, регулирующих процесс и механизмы исполнения положений и требований к системе обеспечения информационной безопасности государства.

**Концепция национальной безопасности Российской Федерации**

В настоящее время в России все большее внимание уделяется вхождению в информационное общество. Но пока не существует ни отдельного Российской Федерации органа исполнительной власти, создающего и проводящего информационную политику, ни, тем более, единого властного органа(по примеру США или Германии), который мог бы объединить все функции, связанные с обеспечением информационной безопасности, реализация которых в настоящее время рассредоточена между Федеральной службой безопасности(ФСБ), Федеральной службой охраны(ФСО), Федеральной службой по техническому и экспортному контролю(ФСТЭК), Министерством обороны, Министерством связи.

Основы государственной политики Российской Федерации в области информатизации и обеспечения информационной безопасности сформулированы в **Концепции национальной безопасности Российской Федерации**, утвержденной Указом Президента Российской Федерации от 17 декабря 1997 г. № 1300 (в редакции Указа Президента Российской Федерации от 10 января 2000 г. № 24), и **Доктрине информационной безопасности Российской Федерации**, утвержденной Президентом Российской Федерации 6 декаьря 2016 г.

Концепция национальной безопасности Российской Федерации отражает систему взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности. В ней сформулировано понятие национальных интересов России в информационной сфере. Это — соблюдение конституционных прав и свобод граждан в области получения информации и пользования ею, развитие современных телекоммуникационных технологий, защита государственных информационных ресурсов от несанкционированного доступа. (Следует сразу оговориться, что подобное сужение понимания национальных интересов до защиты лишь государственных информационных ресурсов и только от несанкционированного доступа непонятно и не может являться приемлемым ни с какой точки зрения, тем более, с точки зрения бизнеса.) В Концепции отмечается усиление угроз национальной безопасности Российской Федерации в информационной сфере. Серьезную опасность, по мнению авторов Кон­цепции, представляют собой стремление ряда стран к доминиро­ванию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормаль­ного функционирования информационных и телекоммуникаци­онных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Очевидно, что перечень угроз в Концепции явно перекрывает область обозначенных национальных интересов, что указывает на слабую проработанность в ней вопросов обеспечения информационной безопасности, поскольку сформулированные в ней важнейшие задачи обеспечения информационной безопасности Российской Федерации, а именно:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;

- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое ин­формационное пространство;

- противодействие угрозе развязывания противоборства в информационной сфере,

очевидно не соотнесены с национальными интересами в информационной сфере.

**Доктрина информационной безопасности Российской Федерации**

Доктрина информационной безопасности Российской Федерации, представляющая собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации, очевидным образом выправляет указанные недостатки Концепции национальной безопасности.

Под информационной безопасностью Российской Федерации в Доктрине понимается состояние защищенности ее нацио­нальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

По мнению разработчиков Доктрины, интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не зап­рещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность, интересы общества в информационной сфере — в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России, а интересы государства в информационной сфере — в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обес­печении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Очевидно, что области национальных интересов России, обозначенные в Концепции национальной безопасности и Доктрине информационной безопасности, как минимум, не совпадают и, более того, значительно расходятся, причем в Концепции они обозначены гораздо уже.

В Доктрине подчеркивается, что обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Утверждается, что воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

- система государственной статистики;

- кредитно-финансовая система;

- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государ­ства в сфере экономики;

- системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

При анализе угроз информационной безопасности Российской Федерации в данной сфере констатируется, что переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и контроля за процессами ее передачи и обработки со стороны иностранных спецслужб. Критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости России от иностранных государств. Серьезную угрозу для нормального функционирования экономики в целом представляют компью­терные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций. Недостаточность нормативной право­вой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, потребительских свойствах про­изводимых ими товаров и услуг, результатах их хозяйствен­ной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее иска­жение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

В качестве основных мер по обеспечению информационной безопасности Российской Федерации в сфере экономики Доктриной провозглашаются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- коренная перестройка системы государственной статис­тической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;

- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистичес­кой, финансовой, биржевой, налоговой, таможенной информации;

- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;

- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

- совершенствование методов отбора и подготовки персона­ла для работы в системах сбора, обработки, хранения и передачи экономической информации.

Однако в целом Доктрину нельзя назвать образцом системно­го подхода к решению обозначенных в ней проблем. Она во многом плохо структурирована, эклектична, содержит смесь разноуровневых вопросов и методов их решения. Более того, если учесть, что практически во всех мировых культурах безо­пасность понимается, как ощущение защищенности от различ­ного рода опасностей, то понятие информационной безопасности страны должно совпадать с ощущением защищенности от при­менения целенаправленного информационного воздействия как извне, так и внутри страны, направленного на причинение ущерба стране. Именно такая постановка проблемы и должна была бы стать ключевой для Доктрины. Однако же в ней разработчиками фактически проблема информационной безопасности во многом подменена проблемой безопасности информации. По мнению многих специалистов, строго формально направление, связан­ное с защитой от целенаправленного информационного воздействия, в Доктрине, как самостоятельная составляющая, отсутствует.

Все это указывает на отсутствие системной проработанности вопросов обеспечения информационной безопасности в Российской Федерации в концептуальных документах, притом, однако, что такие документы создаются, существуют, но во многом, несмотря на важность и остроту ставящихся в них вопросов, яв­ляются невостребованными и слабосвязанными с правовыми актами и нормативными документами.

**Концепция использования информационных технологий**

**Концепция использования ИТ в деятельности федеральных органов государственной власти России до 2010 г.** разработана Министерством информационных технологий и связи. Ее целью является определение основных приоритетов, принципов и направлений реализации единой государственной политики в сфере использования ИТ в деятельности федеральных органов государственной власти. В результате реализации Концепции ожидается формирование эффективной системы предоставления государственных услуг на основе использования ИТ.

В качестве предпосылок создания Концепции отмечается, что в настоящее время уже успешно реализуются проекты внедрения информационных систем (ИС) в сфере электронного документооборота, управления материально-техническими, финансовыми и кадровыми ресурсами, а также проекты интеграции государственных информационных ресурсов между собой в рамках внедрения электронных административных регламентов предоставления государственных услуг.

В Концепции поставлен ряд задач, решение которых позволит повысить эффективность использования ИТ. Среди этих задач имеются и связанные с защитой информации:

1. Обеспечение информационной безопасности деятельности федеральных органов государственной власти (ОГВ) и элементов информационно-технологической инфраструктуры.

2. Развитие единой защищенной телекоммуникационной инфраструктуры для государственных нужд, системы удостоверяющих центров в области электронной цифровой подписи (ЭЦП) и электронной среды взаимодействия, обеспечивающей эффективный межведомственный информационный обмен.

3. Разработка стандартов в сфере использования ИТ в деятельности федеральных органов госвласти, создание государственных ИС, их интеграции и совместного использования в рамках создания общего информационного пространства федеральных органов власти.

4. Защита интеллектуальной собственности, недопущение использования в деятельности федеральных органов власти ПО, не имеющего соответствующей лицензионной поддержки.

Концепция определяет основные приоритеты в следующих областях:

-социально-экономического развития;

- государственного управления;

- обеспечения информационной открытости;

**- информационной безопасности;**

- формирования информационного пространства и защищенной информационной среды федеральных органов власти;

- разработки единых требований к основным элементам информационно-технологического обеспечения;

- создания общегосударственных информационных ресурсов;

- совершенствования нормативной правовой базы в области ИТ и др.

В сфере ***информационной безопасности*** должны быть развиты основные положения Доктрины информационной безопасности Российской Федерации. Предлагается применить единые требования защиты информации от НСД или изменений, воздействия компьютерных атак и вирусов, а также требования использования сертифицированных отечественных средств предупреждения и обнаружения компьютерных атак и защиты информации, разрабатываемых и производимых организациями, получившими в установленном порядке необходимые лицензии.

Для ИС и ресурсов, содержащих сведения, составляющие гостайну, считать обязательным применение криптографических средств ЗИ.

Контроль использования и защита государственных информационных ресурсов и систем от НСД должны обеспечиваться на основе создания комплексной системы мониторинга и учета операций при работе с государственными ИС и ресурсами.

В качестве основных направлений повышения уровня защищенности объектов общей информационно-технологической инфраструктуры выделяются следующие:

1. Обеспечение комплексного подхода к решению задач ИБ с учетом необходимости ее дифференцирования на разных уровнях власти.

2. Разработка модели угроз ИБ.

3. Определение технических требований и критериев определения критических объектов информационно-технологической инфраструктуры, создание реестра критически важных объектов, разработка мер по их защите и средств надзора за соблюдением соответствующих требований.

4. Обеспечение эффективного мониторинга состояния ИБ.

5. Совершенствование нормативной правовой и методической базы в области защиты государственных ИС и ресурсов, формирование единого порядка согласования ТЗ на обеспечение ИБ.

6. Проведение уполномоченными федеральными органами власти аттестации государственных ИС и ресурсов, используемых в органах власти и контроль их соответствия требованиям ИБ.

7. Создание физически обособленного телекоммуникационного сегмента специального назначения, обеспечивающего возможность обмена в электронном виде информацией, содержащей государственную тайну, ограниченным кругом органов власти.

8. Развитие средств ЗИ, систем обеспечения безопасности электронного документооборота, системы контроля действий госслужащих при работе с информацией, развитие и совершенствование защищенных средств обработки информации общего применения, систем удостоверяющих центров в области ЭЦП, а также систем их сертификации и аудита.

Определены девять основополагающих принципов *государственной политики* в области использования ИТ.

Среди них отметим такие как:

- подчинение процессов использования ИТ решению задач обеспечения обороноспособности и национальной безопасности страны;

- согласованность нормативной правовой и методической базы в сфере ИТ на всех уровнях;

- унификация элементов информационно-технологической инфраструктуры, использование типовых решений при создании ИС.

В сфере формирования *общего информационного пространства* и защищенной информационной среды предполагается развитие:

- единой защищенной телекоммуникационной инфраструктуры для государственных нужд;

- системы удостоверяющих центров в области ЭЦП уполномоченных лиц государственной власти;

- электронной среды взаимодействия органов власти.

Единая защищенная телекоммуникационная инфраструктура для государственных нужд создается на основе интеграции существующих и создаваемых телекоммуникационных сетей органов власти всех уровней. Она должна обеспечивать гарантированный уровень функциональности государственных ИС, ресурсов и технологий.

Система удостоверяющих центров в области ЭЦП должна включать:

- федеральный удостоверяющий центр в области ЭЦП;

- удостоверяющие центры федеральных органов власти и их территориальных подразделений;

- уполномоченный федеральный орган исполнительной власти в области использования ЭЦП, ведущий единый государственный реестр сертификатов ключей подписей (СКП) удостоверяющих центров и реестр СКП уполномоченных лиц органов власти.

Электронная среда взаимодействия органов власти должна обеспечивать интеграцию и совместную работу государственных ИС, автоматизированный обмен данными между ними на межведомственном уровне, на основе создания:

- реестра, содержащего описание государственных ИС и ресурсов, способов и интерфейсов взаимодействия с ними, а также используемых схем организации обмена данными;

- инфраструктуры и механизмов маршрутизации, трансформации и гарантированной доставки сообщений и данных между отдельными государственными ИС.

*В области разработки единых требований* к основным элементам информационно-технологического обеспечения предполагается формирование общих стандартов создания, интеграции и совместного использования типовых элементов информационно-технологической инфраструктуры. Общие стандарты определяют общие требования и порядок выполнения работ по проектированию, реализации, внедрению, эксплуатации и развитию типовых элементов информационно-технологической инфраструктуры.

Стандарты утверждаются для следующих типовых элементов информационно-технологической инфрастуктуры органов власти:

- системы взаимодействия с гражданами и организациями, обеспечивающими предоставление им справочной информации, в том числе и через Интернет;

- учетные системы;

- системы межведомственного взаимодействия и обмена информацией;

- системы управления государственными ресурсами;

- офисные системы, используемые сотрудниками органов власти для подготовки документов и обмена информацией;

- информационно-аналитические системы, обеспечивающие сбор, обработку, хранение и анализ данных о состоянии закрепленных за органами власти сфер государственного регулирования и результатах выполнения ими основных задач и функций;

- системы управления электронными архивами документов;

- системы управления проектами;

- системы ИБ;

- системы управления эксплуатацией.

В целях интеграции, совместного использования с информационного взаимодействия государственных ИС на межведомственном уровне утверждаются:

- стандарты метаданных информационных объектов;

- стандарты описания государственных ИС и ресурсов;

- стандарты предоставления информационных сервисов;

- стандарты информационного электронного обмена и сетевого взаимодействия.

Для координации и согласования действий органов власти в этой сфере предлагается создать межведомственный координационный (совещательный) орган при Министерстве информационных технологий и связи.

В сфере создания *общегосударственных ресурсов* предлагается в их состав включать: регистры, кадастры, классификаторы.

В сфере обеспечения *защиты интеллектуальной собственности* в области ИТ ответственность за соблюдение соответствующих нормативных актов возлагается на федеральные органы власти. Предлагается вести ускоренную разработку отечественных программно-технических средств, свободного распространения типовых решений, разработанных за счет федерального бюджета. Необходимо обеспечить открытость и возможность анализа кода закупаемого готового ПО зарубежного производства.

**Нормативно-правовые акты Российской Федерации**

**Кодексы**

**Гражданский кодекс Российской Федерации** (Часть первая от 30 ноября 1994 г. № 51-ФЗ, Часть вторая от 26 января 1996 г. № 14-ФЗ, Часть третья от 26 ноября 2001 г. № 146-ФЗ, с изменениями и дополнениями, Часть четвертая от 18.12.2006).

Определяет правовое положение участников гражданского оборота, основания возникновения и порядок осуществления права собственности и других вещных прав, исключительных прав на результаты интеллектуальной деятельности (интеллектуальной собственности), регулирует договорные и иные обязательства, а также другие имущественные и связанные с ними личные неимущественные отношения, основанные на равенстве, автономии воли и имущественной самостоятельности их участников.

Участниками регулируемых гражданским законодательством отношений являются граждане и юридические лица. В регулируемых гражданским законодательством отношениях могут участвовать также Российская Федерация, субъекты Российской Федерации и муниципальные образования.

Впервые в правовой практике России информация как один из объектов права определяется в "**Гражданском кодексе Российской Федерации** ". **Ст. 128** (Виды объектов гражданских прав) гласит: "К объектам гражданских прав относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права; работы и услуги; информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность)…".

**Статья 138**. **Интеллектуальная собственность**.

В случаях и в порядке, установленных настоящим Кодексом и другими законами, признается исключительное право (интеллектуальная собственность) гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.).

Использование результатов интеллектуальной деятельности и средств индивидуализации, которые являются объектом исключительных прав, может осуществляться третьими лицами только с согласия правообладателя.

Данная статья определяет, что результаты интеллектуальной деятельности, как и приравненные к ним в правовом режиме средства индивидуализации товаров и их изготовителей, относятся к категории нематериальных объектов. Духовная природа таких объектов обусловливает основные особенности правового регулирования отношений, связанных с использованием и защитой исключительных прав. К этим отношениям неприменимы нормы о праве собственности, относящиеся к вещным правам.

Охрана интеллектуальной собственности в России гарантируется нормами статьи 44 Конституции. Законодательство об интеллектуальной собственности входит в сферу исключительной компетенции Федерации (пункт "о" статьи 71 Конституции).

Здесь ГК, устанавливая общий принцип закрепления исключительных прав за гражданином или юридическим лицом на объекты интеллектуальной собственности, отсылает к специальным законам, определяющим условия возникновения, использования, защиты этих прав, а также сроки их действия. В частности, исключительные права делятся на несколько групп, для которых установлен различный правовой режим использования и защиты. Традиционно выделяются две основные группы: "промышленные права" ("промышленная собственность") и "художественные права" ("художественная собственность"), к которым примыкают "смежные" права исполнителей, производителей фонограмм, организаций эфирного и кабельного вещания. Технический прогресс способствует расширению сферы исключительных прав, включению в нее новых видов нематериальных объектов (топологий ИМС, программ для ЭВМ, баз данных и др.).

Исключительные права на объекты промышленной собственности удостоверяются охранными документами: патентами на изобретения и промышленные образцы, свидетельствами на полезные модели, товарные знаки, наименования мест происхождения. Патенты и свидетельства выдаются в соответствии с установленной процедурой патентным ведомством Российской Федерации на основе акта государственной регистрации заявленных объектов.

Охрана исключительных прав на художественную собственность (произведения литературы, науки и искусства), а также объекты смежных прав и топологий ИМС не требует государственной регистрации или иного оформления. Основанием для защиты служит сам факт создания произведения в форме, доступной для восприятия другими лицами, что не препятствует их регистрации по желанию правообладателя. В частности, патентное ведомство ведет соответствующие регистрационные реестры.

**Статья 139***.* **Служебная и коммерческая тайна.**

1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Данная статья предусматривает защиту прав обладателя сведений, для определения которых применено широкое понятие "информация", не подпадающих под охрану норм патентного, авторско-правового или иного специального законодательства. Правила статьи распространяются также на охраноспособные решения (изобретения, полезные модели и др.), не запатентованные правообладателем по каким-либо, как правило, экономическим, мотивам.

Статья не раскрывает содержание сведений, составляющих служебную или коммерческую тайну, и не приводит их перечень. Установлен только один общий признак, которым должна обладать охраняемая информация – "коммерческая ценность", т.е. способность быть объектом рыночного оборота. Условием предоставления защиты служит принятие правообладателем всех необходимых мер для обеспечения ее конфиденциальности. При соблюдении этих требований под правила статьи подпадают, таким образом, любые знания, включая практический опыт специалистов, применяемые не только в производстве, но и в других областях хозяйственной деятельности: торговле, маркетинге, менеджменте, иных управленческих услугах.

Нормы о коммерческой тайне содержатся и в ряде других российских законов, в частности в законе «о коммерческой тайне». Права на коммерческую тайну действуют, пока соблюдаются условия их защиты. Признание тех или иных сведений конфиденциальными является прерогативой правообладателя. Исключения из этой общей нормы устанавливаются законом или иным правовым актом.

Вместе с тем, в некоторых источниках высказывается сомнение в правомерности распространения условий охраны коммерческой тайны на служебную. Это разноплановые понятия. Сохранение в тайне служебной информации, как правило, не обусловлено ее коммерческой ценностью (хотя такая информация и может содержать сведения коммерческого характера). Запрет ее разглашения основывается на законодательстве, регламентирующем отдельные сферы деятельности (например, Законы РФ "О страховании", "О связи" и др.). Определенные категории работников такой сферы деятельности обязаны сохранять в тайне сведения, к которым они имеют доступ в связи с выполняемой работой (банковские служащие, работники связи, налоговые инспекторы, страховые агенты, врачи и др.).

Закрепление исключительных прав обладателя коммерческой тайны имеет свои особенности. Эта защита основывается на *системе конфиденциальности*, ее нарушение влечет прекращение прав. Условием же предоставления охраны изобретениям, полезным моделям, промышленным образцам, напротив, служит их *опубликование*.

Охраняемая информация может быть использована другими лицами при соблюдении двух условий: получения самой информации законным путем и получения разрешения правообладателя на такое использование ("беспатентная лицензия"). Отношения между правообладателем (лицензиаром) и пользователем (лицензиатом) оформляются лицензионным договором. Элементы лицензионного договора могут включаться в другие гражданско-правовые договоры (на выполнение научно-исследовательских, опытно-конструкторских и технологических работ, подряда, о создании акционерного общества и др.).

Защита служебной и коммерческой тайны от неправомерных посягательств может осуществляться на основе норм гражданского, административного либо уголовного права. В качестве основного гражданско-правового способа защиты статья указывает возмещение причиненных правообладателю убытков. При определении их размера может быть учтен как реальный ущерб, так и упущенная выгода.

Существенным новшеством в ГК является введение *имущественной ответственности* лица перед своим *работодателем* за разглашение служебной или коммерческой тайны, что предполагает необходимость включения соответствующих условий в трудовое соглашение. Вместе с тем, санкции за нарушение служебной тайны устанавливаются также нормами законов о соответствующих видах деятельности.

**Статья 771. Конфиденциальность сведений, составляющих предмет договора.**

1. Если иное не предусмотрено договорами на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, стороны обязаны обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов. Объем сведений, признаваемых конфиденциальными, определяется в договоре.

2. Каждая из сторон обязуется публиковать полученные при выполнении работы сведения, признанные конфиденциальными, только с согласия другой стороны.

Данная статья определяет, что обязанности сторон по обеспечению конфиденциальности относятся в практике к одним из основных договорных обязательств. Результаты НИОКР не могут быть иначе защищены от незаконного использования третьими лицами. Кроме того, преждевременное разглашение может препятствовать патентной защите охраноспособных технических решений.

**Состав и объем конфиденциальной информации** определяется сторонами. В нее включаются сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них, а также любые другие сведения научного, технического, экономического, организационного характера, которые могут быть отнесены к коммерческой тайне. Эти сведения должны быть неизвестны третьим лицам, что служит предпосылкой их коммерческой ценности, и закрыты для доступа третьих лиц на законном основании.

Нарушением обязательств по обеспечению конфиденциальности признается не только разглашение и прямая передача подобных сведений одной из сторон другим заинтересованным пользователям без согласия партнера, но и непринятие мер к их охране, исключающих свободный доступ к сведениям и возможность их утечки. К таким мерам следует отнести, в частности, ознакомление сотрудников (исполнителя и заказчика), участвующих в выполнении договорных работ и имеющих доступ к информации, с правилами соблюдения конфиденциальности. Необходимые условия могут быть включены в трудовой договор (контракт), учитывая, что обязанность работника, разгласившего служебную или коммерческую тайну, возместить причиненные работодателю убытки наступает, если работник это сделал вопреки трудовому договору.

Правила статьи относятся как к сведениям, которыми стороны обладают на момент заключения договора, так и к полученным в процессе выполнения работ.

Вопрос о форме, времени, объеме и целях публикации таких сведений должен решаться только по согласованию между сторонами – заказчиком и исполнителем, исходя из оговоренных ими условий и способов использования созданных научных и производственных новшеств, а также целей их опубликования.

Наиболее широким способом разглашения является публикация в средствах массовой информации. В то же время стороны могут быть заинтересованы в опубликовании информации в рекламных или иных целях, например, для закрепления научного приоритета и т.п.

**Статья 857*.* Банковская тайна.**

1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом.

3. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

Данная статья определяет обязанность хранить банковскую тайну, которая распространяется на кредитные, аудиторские организации и Центральный банк Российской Федерации (ЦБ РФ).

Эта обязанность носит личный характер. Т.е. перечень лиц, обязанных сохранять банковскую тайну, включает в себя всех служащих перечисленных организаций, независимо от их должности и от того, входит ли работа с охраняемыми сведениями в круг их непосредственных служебных обязанностей. Если о банковских операциях узнает частное лицо (из разговоров, писем и т.п.), то оно не обязано соблюдать тайну.

В **состав банковской тайны**входят сведения о счетах и вкладах, операциях по счетам и вкладам, сведений о клиентах и корреспондентах, а также иной информации, устанавливаемой кредитной организацией, если это не противоречит федеральному закону ( «О банках и банковской деятельности»). Следовательно, кредитная организация не обязана хранить в тайне сведения о контрагентах своих клиентов, а также другую информацию, не имеющую непосредственного отношения к банковскому счету (кроме сведений о клиенте), если она не взяла на себя такие обязательства. Тайна распространяется однако на движение вкладов (размер, время и сумма поступления или изъятия, от кого и по каким основаниям поступают суммы и пр.). Сведения, составляющие банковскую тайну, должны быть получены кредитной организацией в процессе осуществления ею банковских операций и других сделок, предусмотренных Законом о банках.

Помимо указанных сведений ЦБ РФ не вправе разглашать данные о счетах, вкладах, конкретных сделках и операциях, полученных им из отчетов кредитных организаций или в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Аудиторские организации не вправе раскрывать третьим лицам сведения об операциях, счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

Пределы раскрытия банковской тайны определяются законодательством. Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются им самим (а также их представителям), судам и арбитражным судам (судьям), Счетной палате РФ, органам федеральной налоговой службы, таможенным органам РФ, следственным органам – в случаях, предусмотренных законодательными актами об их деятельности, а также по решению суда.

В числе органов и должностных лиц, которым должны быть предоставлены сведения, составляющие банковскую тайну, отсутствуют судебные приставы-исполнители. Они вправе получать интересующие их сведения через налоговые органы.

За разглашение банковской тайны ЦБ РФ, кредитные и аудиторские организации могут быть привлечены к ответственности в форме возмещения убытков. Их должностные лица и иные работники несут уголовную ответственность.

**Статья 946*.* Тайна страхования.**

Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными статьей 139 или статьей 150 настоящего Кодекса.

Данная статья вводит понятие **тайны страхования**. К ней относятся ставшие известными страховщику сведения, составляющие служебную и/или коммерческую тайну страхователей, выгодоприобретателей и застрахованных лиц, а также личную и/или семейную тайну этих лиц и, кроме того, сведения о здоровье и имущественном положении этих лиц.

Ответственность страховщика как юридического лица за разглашение тайны страхования носит общий характер, однако она наступает только, если использование или разглашение полученных страховщиком сведений является незаконным. Иными словами, ответственность за использование или разглашение тайны страхования не может быть возложена на страховщика, если какой-либо закон не предусматривает запрет на использование или разглашение этих сведений.

Статья играет такую же роль и при защите тайны страхования от ее несанкционированного корыстного использования и распространения работниками страховщика, поскольку ответственность работника страховщика за ее разглашение или за несанкционированное корыстное использование также наступает только, если эти действия являются незаконными.

С 1 января 2008 года вступила в силу **Часть IV Гражданского кодекса РФ**. Эта часть регулирует отношения в сфере интеллектуальной собственности.

**Налоговый кодекс Российской Федерации** (Часть первая от 31 июля 1998 г. № 146-ФЗ, Часть вторая от 5 августа 2000 г. № 117-ФЗ, с изменениями и дополнениями).

Кодекс устанавливает *систему налогов и сборов*, взимаемых в федеральный бюджет, а также общие принципы налогообложения и сборов в Российской Федерации, в том числе: виды налогов и сборов, взимаемых в Российской Федерации; основания возникновения (изменения, прекращения) и порядок исполнения обязанностей по уплате налогов и сборов; принципы установления, введения в действие и прекращения действия ранее введенных налогов и сборов субъектов Российской Федерации и местных налогов и сборов; права и обязанности налогоплательщиков, налоговых органов и других участников отношений, регулируемых законодательством о налогах и сборах; формы и методы налогового контроля; ответственность за совершение налоговых правонарушений; порядок обжалования актов налоговых органов и действий (бездействия) их должностных лиц.

**Статья 32** Кодекса определяет обязанность налоговых органов *бесплатно информировать* (в том числе в письменной форме) налогоплательщиков о действующих налогах и сборах, законодательстве о налогах и сборах и принятых в соответствии с ним нормативных правовых актах, порядке исчисления и уплаты налогов и сборов, правах и обязанностях налогоплательщиков, полномочиях налоговых органов и их должностных лиц, а также предоставлять формы налоговой отчетности и разъяснять порядок их заполнения.

**Статья 102** Кодекса устанавливает понятие ***налоговой тайны***. Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений:

- разглашенных налогоплательщиком самостоятельно или с его согласия;

- об идентификационном номере налогоплательщика;

- о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения;

- предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация.

**Трудовой кодекс Российской Федерации** (от 30 декабря 2001 г. № 197-ФЗ, с изменениями и дополнениями).

Кодекс устанавливает государственные гарантии трудовых прав и свобод граждан, благоприятных условий труда, защиты прав и интересов работников и работодателей.

**Глава 14** Кодекса регулирует вопросы, связанные с защитой персональных данных работника.

**Семейный кодекс Российской Федерации**

(от 29 декабря 1995 г. № 223-ФЗ, с изменениями и дополнениями).

Семейное законодательство устанавливает условия и порядок вступления в брак, прекращения брака и признания его недействительным, регулирует личные неимущественные и имущественные отношения между членами семьи: супругами, родителями и детьми (усыновителями и усыновленными), а в случаях и в пределах, предусмотренных семейным законодательством, между другими родственниками и иными лицами, а также определяет формы и порядок устройства в семью детей, оставшихся без попечения родителей.

**Статья 139** Кодекса определяет *тайну усыновления ребенка*:

Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка.

**Кодекс Российской Федерации об административных правонарушениях**

(от 30 декабря 2001 г. № 195-ФЗ, с изменениями и дополнениями).

Задачами законодательства об административных правонарушениях являются защита личности, охрана прав и свобод человека и гражданина, охрана здоровья граждан, санитарно-эпидемиологического благополучия населения, защита общественной нравственности, охрана окружающей среды, установленного порядка осуществления государственной власти, общественного порядка и общественной безопасности, собственности, защита законных экономических интересов физических и юридических лиц, общества и государства от административных правонарушений, а также предупреждение административных правонарушений.

В Кодексе Российской Федерации об административных правонарушениях вопросам информационной безопасности и интеллектуальной собственности посвящены следующие главы и статьи.

**Глава 5. Административные правонарушения, посягающие на права граждан.**

***Статья 5.39****.* Отказ в предоставлении гражданину информации.

Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации.

**Глава 8. Административные правонарушения в области охраны окружающей природной среды и природопользования.**

***Статья 8.5****.* Сокрытие или искажение экологической информации.

Сокрытие, умышленное искажение или несвоевременное сообщение полной и достоверной информации о состоянии окружающей природной среды и природных ресурсов, об источниках загрязнения окружающей природной среды и природных ресурсов или иного вредного воздействия на окружающую природную среду и природные ресурсы, о радиационной обстановке, а равно искажение сведений о состоянии земель, водных объектов и других объектов окружающей природной среды лицами, обязанными сообщать такую информацию.

**Глава 13. Административные правонарушения в области связи и информации.**

***Статья 13.11****.* Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

***Статья 13.12****.* Нарушение правил защиты информации.

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну).

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну).

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну.

***Статья 13.13****.* Незаконная деятельность в области защиты информации.

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна).

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну без лицензии.

***Статья 13.14****.* Разглашение информации с ограниченным доступом.

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

***Статья 13.15****.* Злоупотребление свободой массовой информации.

Изготовление и (или) распространение теле-, видео-, кинопрограмм, документальных и художественных фильмов, а также относящихся к специальным средствам массовой информации информационных компьютерных файлов и программ обработки информационных текстов, содержащих скрытые вставки, воздействующие на подсознание людей и (или) оказывающие вредное влияние на их здоровье.

***Статья 13.16****.* Воспрепятствование распространению продукции средства массовой информации.

Воспрепятствование осуществляемому на законном основании распространению продукции средства массовой информации либо установление незаконных ограничений на розничную продажу тиража периодического печатного издания.

***Статья 13.17****.* Нарушение правил распространения обязательных сообщений.

Нарушение правил распространения обязательных сообщений.

***Статья 23.45****.* Органы, осуществляющие контроль за обеспечением защиты государственной тайны.

1. Органы, осуществляющие контроль за обеспечением защиты государственной тайны, рассматривают дела об административных правонарушениях, предусмотренных частями 3 и 4 статьи 13.12, частью 2 статьи 13.13 настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органов, указанных в части 1 настоящей статьи, вправе:

1) руководитель федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности Российской Федерации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители;

2) руководитель федерального органа исполнительной власти, уполномоченного в области обороны, его заместители;

3) руководитель федерального органа исполнительной власти, уполномоченного в области внешней разведки, его заместители;

4) руководитель федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители;

5) руководители подразделений федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности Российской Федерации, обороны Российской Федерации, внешней разведки, противодействия техническим разведкам и технической защиты информации, осуществляющих лицензирование видов деятельности, которые связаны с использованием и защитой сведений, составляющих государственную тайну.

**Уголовный кодекс Российской Федерации**

(от 13 июня 1996 г. № 63‑ФЗ, с изменениями и дополнениями).

Устанавливает основание и принципы уголовной ответственности, определяет, какие опасные для личности, общества или государства деяния признаются преступлениями, и устанавливает виды наказаний и иные меры уголовно-правового характера за совершение преступлений.

В Уголовном кодексе Российской Федерации вопросам безопасности информации и интеллектуальной собственности посвящены следующие главы и статьи.

**Глава 19. Преступления против конституционных прав и свобод человека и гражданина.**

***Статья 137****.* Нарушение неприкосновенности частной жизни.

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан.

2. Те же деяния, совершенные лицом с использованием своего служебного положения.

***Статья 138****.* Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации.

3. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.

***Статья 140****.* Отказ в предоставлении гражданину информации.

Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан.

***Статья 144****.* Воспрепятствование законной профессиональной деятельности журналистов.

1. Воспрепятствование законной профессиональной деятельности журналистов путем принуждения их к распространению либо к отказу от распространения информации.

2. То же деяние, совершенное лицом с использованием своего служебного положения.

***Статья 146****.* Нарушение авторских и смежных прав.

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб (свыше 100 МРОТ) автору или иному правообладателю.

2. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере.

3. Деяния, предусмотренные частью второй настоящей статьи, если они совершены:

неоднократно;

группой лиц по предварительному сговору или организованной группой;

в особо крупном размере (свыше 500 МРОТ);

лицом с использованием своего служебного положения.

***Статья 147****.* Нарушение изобретательских и патентных прав.

1. Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой.

**Глава 20. Преступления против семьи и несовершеннолетних.**

***Статья 155****.* Разглашение тайны усыновления (удочерения).

Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну, либо иным лицом из корыстных или иных низменных побуждений.

**Глава 22. Преступления в сфере экономической деятельности.**

***Статья 155****.* Мошенничество.

Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

***Статья 163****.*Вымогательство.

Вымогательство, то есть требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких.

***Статья 165****.* Причинение имущественного ущерба путем обмана или злоупотребления доверием.

Причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием при отсутствии признаков хищения.

***Статья 179****.* Принуждение к совершению сделки или к отказу от ее совершения.

Принуждение к совершению сделки или к отказу от ее совершения под угрозой применения насилия, уничтожения или повреждения чужого имущества, а равно распространения сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего или его близких, при отсутствии признаков вымогательства.

***Статья 180****.* Незаконное использование товарного знака.

1. Незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров, если это деяние совершено неоднократно или причинило крупный ущерб.

2. Незаконное использование предупредительной маркировки в отношении не зарегистрированного в Российской Федерации товарного знака или наименования места происхождения товара, если это деяние совершено неоднократно или причинило крупный ущерб.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой.

***Статья 182****.* Заведомо ложная реклама.

Использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей (исполнителей, продавцов), совершенное из корыстной заинтересованности и причинившее значительный ущерб.

***Статья 183****.* Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия.

***Статья 185****.* Злоупотребления при эмиссии ценных бумаг.

1. Внесение в проспект эмиссии ценных бумаг заведомо недостоверной информации, утверждение содержащего заведомо недостоверную информацию проспекта эмиссии или отчета об итогах выпуска ценных бумаг, а равно размещение эмиссионных ценных бумаг, выпуск которых не прошел государственную регистрацию, если эти деяния причинили крупный (свыше 2000 МРОТ) ущерб гражданам, организациям или государству.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой.

***Статья 185.1****.* Злостное уклонение от предоставления инвестору или контролирующему органу информации, определенной законодательством Российской Федерации о ценных бумагах.

Злостное уклонение от предоставления информации, содержащей данные об эмитенте, о его финансово-хозяйственной деятельности и ценных бумагах, сделках и иных операциях с ценными бумагами, лица, обязанного обеспечить указанной информацией инвестора или контролирующий орган, либо предоставление заведомо неполной или ложной информации, если эти деяния причинили крупный ущерб гражданам, организациям или государству.

***Статья 186****.* Изготовление или сбыт поддельных денег или ценных бумаг.

1. Изготовление в целях сбыта или сбыт поддельных банковских билетов Центрального банка Российской Федерации, металлической монеты, государственных ценных бумаг или других ценных бумаг в валюте Российской Федерации либо иностранной валюты или ценных бумаг в иностранной валюте.

2. Те же деяния, совершенные в крупном размере либо лицом, ранее судимым за изготовление или сбыт поддельных денег или ценных бумаг.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой.

***Статья 187****.* Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

1. Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами.

2. Те же деяния, совершенные неоднократно или организованной группой.

***Статья 189****.* Незаконный экспорт технологий, научно-технической информации и услуг, сырья, материалов и оборудования, которые могут использоваться при создании оружия массового поражения, вооружения и военной техники.

Незаконный экспорт технологий, научно-технической информации и услуг, сырья, материалов и оборудования, которые могут быть использованы при создании оружия массового поражения, средств его доставки, вооружения и военной техники и в отношении которых установлен специальный экспортный контроль.

**Глава 23. Преступления против интересов службы в коммерческих и иных организациях.**

***Статья 201****.* Злоупотребление полномочиями.

1. Использование лицом, выполняющим управленческие функции в коммерческой или иной организации, своих полномочий вопреки законным интересам этой организации и в целях извлечения выгод и преимуществ для себя или других лиц либо нанесения вреда другим лицам, если это деяние повлекло причинение существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

2. То же деяние, повлекшее тяжкие последствия.

***Статья 202****.* Злоупотребление полномочиями частными нотариусами и аудиторами.

1. Использование частным нотариусом или частным аудитором своих полномочий вопреки задачам своей деятельности и в целях извлечения выгод и преимуществ для себя или других лиц либо нанесения вреда другим лицам, если это деяние причинило существенный вред правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

2. То же деяние, совершенное в отношении заведомо несовершеннолетнего или недееспособного лица либо неоднократно.

***Статья 203****.*Превышение полномочий служащими частных охранных или детективных служб.

1. Превышение руководителем или служащим частной охранной или детективной службы полномочий, предоставленных им в соответствии с лицензией, вопреки задачам своей деятельности, если это деяние совершено с применением насилия или с угрозой его применения.

2. То же деяние, повлекшее тяжкие последствия.

**Глава 25. Преступления против здоровья населения и общественной нравственности.**

***Статья 237****.*Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.

1. Сокрытие или искажение информации о событиях, фактах или явлениях, создающих опасность для жизни или здоровья людей либо для окружающей среды, совершенные лицом, обязанным обеспечивать население и органы, уполномоченные на принятие мер по устранению такой опасности, указанной информацией.

2. Те же деяния, если они совершены лицом, занимающим государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, а равно главой органа местного самоуправления либо если в результате таких деяний причинен вред здоровью человека или наступили иные тяжкие последствия.

**Глава 28. Преступления в сфере компьютерной информации.**

***Статья 272****.*Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

***Статья 273****.* Создание, использование и распространение вредоносных программ для ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия.

***Статья 274****.* Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

2. То же деяние, повлекшее по неосторожности тяжкие последствия.

**Глава 29. Преступления против основ конституционного строя и безопасности государства.**

***Статья 275****.* Государственная измена.

Государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, совершенная гражданином Российской Федерации.

***Статья 276****.* Шпионаж.

Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Федерации, если эти деяния совершены иностранным гражданином или лицом без гражданства.

***Статья 283****.* Разглашение государственной тайны.

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены.

2. То же деяние, повлекшее по неосторожности тяжкие последствия.

***Статья 284****.* Утрата документов, содержащих государственную тайну.

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий.

**Законы Российской федерации**

В настоящее время в **Государственной думе РФ** за информационную безопасность отвечают три Комитета:

1. Комитет по информационной политике,

2. Комитет по безопасности,

3. Комитет по энергетике, транспорту и связи.

В положении о каждом из этих трех комитетов указано, что он отвечает за информационную безопасность.

Законодательные органы в рамках развития информационного законодательства на практике осуществлял конкретизацию видов и форм представления информации и информационных объектов при регулировании конкретных информационных отношений.

Комплексное исследование процессов в информационной сфере, правовых норм, регулирующих отношения, возникающие в этих процессах, действий, совершаемых с информацией, позволяет установить такие ее особенности и свойства, как:

- свойство физической неотчуждаемости информации. Оно основано на том, что знания не отчуждаемы от человека, их носителя. Исходя из этого при передаче информации от одного лица к другому и юридического закрепления этого факта процедура отчуждения информации должна заменяться передачей прав на ее использование и передаваться вместе с этими правами;

- свойство обособляемости информации. Для включений в оборот информация всегда овеществляется в виде символов, знаков, волн, вследствие этого обособляется от ее производителя (создателя) и существует отдельно и независимо от него. Это подтверждает факт оборотоспособности информации как самостоятельного отдельного объекта правоотношений, в результате чего появляется возможность передачи информации в такой форме от одного субъекта к другому;

- свойство информационной вещи (информационного объекта). Это свойство возникает в силу того, что информация передается и распространяется только на материальном носителе или с помощью материального носителя и проявляется как «двуединство» информации (ее содержания) и носителя, на котором эта информация (содержание) закреплено. Это свойство позволяет распространить на информационную вещь (объект) совместное и взаимосвязанное действие двух институтов — института авторского права и института вещной собственности;

- свойство тиражируемости (распространяемости) информации. Информация может тиражироваться и распространяться в неограниченном количестве экземпляров без изменения ее содержания. Одна и та же информация (содержание) может принадлежать одновременно неограниченному кругу лиц (неограниченный круг лиц может знать содержание этой информации). Отсюда следует, что юридически необходимо закреплять объем прав по исполь­зованию информации (ее содержания) лицами, обладающими такой информацией (обладающими знаниями о содержании информации);

- свойство организационной формы. Информация, находящаяся в обороте, как правило, представляется в документированном виде, т.е. в форме документа. Это могут быть подлинник (оригинал) документа, его копия, массив документов на бумажном или электронном носителе (банк данных или база данных) тоже в виде оригинала или копии, библиотека, фонд документов, архив и т.п. Такое свойство дает возможность юридически закреплять факт «принадлежности» документа конкретному лицу, например закрепив его соответствующей подписью в традиционном или в электронном виде (с помощью электронной цифровой подписи). Это свойство позволяет также относить к информационным вещам (информационным объектам) как отдельные документы, так и сложные организационные информационные структуры;

- свойство экземплярности информации. Это свойство заключается в том, что информация распространяется, как правило, не сама по себе, а на материальном носителе, вследствие чего возможен учет экземпляров информации через учет носителей, содержащих информацию. Понятие экземплярности дает возможность учитывать документированную информацию и тем самым связывать содержательную сторону информации с ее «вещным» обрамлением, т.е. с отображением на носителе, вводить понятие учитываемой копии документа, а отсюда и механизма регистрации информации, в особенности учитывать обращение оригиналов (подлинников) документов. Экземплярность информации уже сегодня активно реализуется при обращении информации ограниченного доступа.

Указанные юридические особенности и свойства должны учитываться при правовом регулировании информационных отношений.

Рассмотрим основные законы в области информационной безопасности, останавливаясь на главных из них.

**Федеральный закон от 8 августа 2001 г. № 128-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями и дополнениями).(** вместо ФЗ от 25 сентября 1998 года № 158-ФЗ**)**

Регулирует отношения, возникающие в связи с осуществлением лицензирования отдельных видов деятельности. Распространяется на все органы государственной власти, органы местного самоуправления, юридические лица и индивидуальных предпринимателей.

Определяет порядок лицензирования и виды деятельности, на осуществление которых требуются лицензии.

В связи с тем, что лицензирование деятельности в отдельных сферах регулируется другими федеральными законами и иными нормативными правовыми актами данный Закон в статье 1 оговаривает, на какие сферы его действие не распространяется:

деятельность кредитных организаций;

деятельность, связанная с защитой государственной тайны;

деятельность в области производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции;

деятельность в области связи;

биржевая деятельность;

деятельность в области таможенного дела;

нотариальная деятельность;

страховая деятельность;

деятельность профессиональных участников рынка ценных бумаг;

осуществление внешнеэкономических операций;

осуществление международных автомобильных перевозок грузов и пассажиров;

приобретение оружия и патронов к нему;

использование результатов интеллектуальной деятельности;

использование орбитально-частотных ресурсов и радиочастот для осуществления телевизионного вещания и радиовещания (в том числе вещания дополнительной информации);

использование природных ресурсов, в том числе недр, лесного фонда, объектов растительного и животного мира;

деятельность, работы и услуги в области использования атомной энергии;

образовательная деятельность.

К *лицензируемым видам деятельности* относятся виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам, законным интересам, здоровью граждан, обороне и безопасности государства, культурному наследию народов Российской Федерации и регулирование которых не может осуществляться иными методами, кроме как лицензированием (**статья 4**).

В целях обеспечения единства экономического пространства на территории Российской Федерации Правительство Российской Федерации в соответствии с определенными Президентом Российской Федерации основными направлениями внутренней политики государства (**статья 5**):

утверждает положения о лицензировании конкретных видов деятельности;

определяет федеральные органы исполнительной власти, осуществляющие лицензирование конкретных видов деятельности;

устанавливает виды деятельности, лицензирование которых осуществляется органами исполнительной власти субъектов Российской Федерации.

Лицензирующие органы осуществляют следующие полномочия:

предоставление лицензий;

переоформление документов, подтверждающих наличие лицензий;

приостановление действия лицензий;

возобновление действия лицензий;

аннулирование лицензий;

ведение реестра лицензий;

контроль за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.

*Перечень* федеральных органов исполнительной власти, осуществляющих лицензирование, утвержден **постановлением Правительства Российской Федерации от 11 февраля 2002 г. № 135.**

Порядок осуществления полномочий лицензирующих органов устанавливается положениями о лицензировании конкретных видов деятельности.

В целях Федерального закона применяются следующие понятия:

*Лицензия* – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

*Лицензируемый вид деятельности* – вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с Федеральным законом.

*Лицензирование* – мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих выдачу лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, аннулированием лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, введением регистра лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании.

*Лицензиат* – юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.

*Лицензионные требования и условия* – совокупность установленных положениями о лицензировании конкретных видов деятельности требований и условий, выполнение которых лицензиатом обязательно при осуществлении лицензируемого вида деятельности.

*Лицензирующие органы* – федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с Федеральным законом.

*Соискатель лицензии* – юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии на осуществление конкретного вида деятельности.

*Реестр лицензий* – совокупность данных о предоставлении лицензий, переоформлении документов, подтверждающих наличие лицензий, приостановлении и возобновлении действия лицензий и об аннулировании лицензий.

Ha каждый вид лицензируемой деятельности (перечень изложен в **статье 17 Закона**) предоставляется лицензия. Вид деятельности, на осуществление которого предоставлена лицензия, может выполняться только получившим лицензию юридическим лицом или индивидуальным предпринимателем.

Деятельность, на осуществление которой лицензия предоставлена федеральным органом исполнительной власти или органом исполнительной власти субъекта Российской Федерации, может осуществляться на всей территории Российской Федерации.

Срок действия лицензии не может быть менее чем *пять лет*. Срок действия лицензии по его окончании может быть продлен по заявлению лицензиата. Положениями о лицензировании конкретных видов деятельности может быть предусмотрено бессрочное действие лицензии.

**Статья 9** Закона определяет перечень документов, предоставляемых соискателем для получения лицензии. При этом указывается, что ряд документов, обязательных для предоставления, могут быть предусмотрены иными нормативными правовыми актами, предусмотренными положениями о лицензировании конкретных видов деятельности.

Не допускается требовать от соискателя лицензии представления документов, не предусмотренных данным Федеральным законом и иными федеральными законами.

Все документы, представленные в соответствующий лицензирующий орган для предоставления лицензии, принимаются по описи, копия которой направляется (вручается) соискателю лицензии с отметкой о дате приема документов указанным органом.

Лицензирующий орган принимает решение о предоставлении или об отказе в предоставлении лицензии в срок, не превышающий сорока пяти дней со дня поступления заявления о предоставлении лицензии со всеми необходимыми документами. Соответствующее решение оформляется приказом лицензирующего органа.

Уведомление о предоставлении лицензии направляется (вручается) соискателю лицензии в письменной форме с указанием реквизитов банковского счета и срока уплаты лицензионного сбора за предоставление лицензии.

В течение трех дней после представления соискателем лицензии документа, подтверждающего уплату лицензионного сбора за предоставление лицензии, лицензирующий орган бесплатно выдает лицензиату документ, подтверждающий наличие лицензии.

За рассмотрение лицензирующим органом заявлений о предоставлении лицензий и за предоставление лицензий уплачивается государственная пошлина в размерах и порядке, которые установлены законодательством Российской Федерации о налогах и сборах.

Основанием отказа в предоставлении лицензии является:

наличие в документах, представленных соискателем лицензии, недостоверной или искаженной информации;

несоответствие соискателя лицензии, принадлежащих ему или используемых им объектов лицензионным требованиям и условиям.

Не допускается отказ в выдаче лицензии на основании величины объема продукции (работ, услуг), производимой или планируемой для производства соискателем лицензии.

Соискатель лицензии имеет право обжаловать в порядке, установленном законодательством Российской Федерации, отказ лицензирующего органа в предоставлении лицензии или его бездействие.

Наряду с обычным порядком вводится и *упрощенный порядок лицензирования*. Он может применяться, если соискатель лицензии заключи л договор страхования гражданской ответственности либо имеет сертификат соответствия осуществляемого им лицензируемого вида деятельности международным стандартам. При применении упрощенного порядка лицензирования срок рассмотрения предоставленных документов составляет не более 15 дней.

Контроль за соблюдением лицензиатом лицензионных требований и условий, определенных положением о лицензировании конкретного вида деятельности, осуществляется лицензирующими органами в пределах их компетенции (**статья 12**).

Лицензирующие органы имеют право:

проводить проверки деятельности лицензиата на предмет ее соответствия лицензионным требованиям и условиям;

запрашивать у лицензиата необходимые объяснения и документы при проведении проверок;

составлять на основании результатов проверок акты (протоколы) с указанием конкретных нарушений;

выносить решения, обязывающие лицензиата устранить выявленные нарушения, устанавливать сроки устранения таких нарушений;

выносить предупреждение лицензиату.

Лицензирующие органы вправе приостанавливать действие лицензии в случае выявления лицензирующими органами неоднократных нарушений или грубого нарушения лицензиатом лицензионных требований и условий (**статья 13**).

Лицензирующий орган обязан установить срок устранения лицензиатом нарушений, повлекших за собой приостановление действия лицензии. Указанный срок не может превышать шесть месяцев. В случае, если в установленный срок лицензиат не устранил указанные нарушения, лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии.

**Статья 17** Закона определяет исчерпывающий перечень лицензируемых видов деятельности (всего 103 наименования). К **защите информации** среди них относятся:

деятельность по распространению шифровальных (криптографических) средств;

деятельность по техническому обслуживанию шифровальных (криптографических) средств;

предоставление услуг в области шифрования информации;

разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

деятельность по технической защите конфиденциальной информации;

разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

деятельность по проведению экспертизы промышленной безопасности;

производство работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений;

деятельность по эксплуатации электрических сетей (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

негосударственная (частная) охранная деятельность;

негосударственная (частная) сыскная деятельность;

публичный показ аудиовизуальных произведений, если указанная деятельность осуществляется в кинозале;

воспроизведение (изготовление экземпляров) аудиовизуальных произведений и фонограмм на любых видах носителей;

аудиторская деятельность.

Здесь также перечислены виды деятельности, по отношению к которым может применяться упрощенный порядок лицензирования. Кроме того, дан перечень видов деятельности, лицензирование которых прекратилось с 1 января 2006 и 2007 годов.

Введение лицензирования иных видов деятельности возможно только путем внесения дополнений в предусмотренный настоящим Федеральным законом перечень видов деятельности, на осуществление которых требуются лицензии.

В связи с рассматриваемой нами областью представляет интерес Постановление Правительства от **29 декабря 2007 г. N 957** **«Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»**(вместо П**остановления от 23 сентября 2002 г. N 691**).

Постановление утверждает:

Положение о лицензировании деятельности **по распространению** шифровальных (криптографических) средств;

Положение о лицензировании деятельности **по техническому обслуживанию** шифровальных (криптографических) средств;

Положение о лицензировании **предоставления услуг** в области шифрования информации;

Положение о лицензировании **разработки, производства** шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Новым является:

1. Положения не распространяются на деятельность для:

- шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну;

- шифровальных (криптографических) средств независимо от их назначения, реализующих симметричные криптографические алгоритмы и обладающих максимальной длиной криптографического ключа **менее** **56 бит**, а также реализующих асимметричные криптографические алгоритмы, основанные либо на разложении на множители целых чисел, либо на вычислении дискретных логарифмов в мультипликативной группе конечного поля, либо на дискретном логарифме в группе, отличной от названной, и обладающих максимальной длиной криптографического ключа **128 бит**;

- беспроводного оборудования, осуществляющего шифрование информации только в радиоканале с максимальной дальностью беспроводного действия без усиления и ретрансляции менее 400 м в соответствии с техническими условиями производителя (за исключением оборудования, используемого на критически важных объектах);

- шифровальных (криптографических) средств, используемых для защиты технологических каналов информационно-телекоммуникационных систем и сетей, не относящихся к критически важным объектам.

2. Уменьшилось число лицензионных требований, но теперь они могут быть дополнены требованиями ФСБ, которые в настоящее время неизвестны.

3. Незначительно изменился перечень представляемых документов.

4. Лицензионный контроль за соблюдением лицензиатом лицензионных требований и условий будет осуществляется в соответствии с Федеральным законом "О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)".

5. Исчезло определение деятельности по техническому обслуживанию.

6. Появился новый пункт о деятельности с нарушением и определение грубого нарушения.

**Федеральный закон от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании".**

Регулирует отношения, возникающие при разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнении работ или оказанию услуг; разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг; оценке соответствия.

Данный закон вступил в силу с 1 июля 2003 г. При этом утратили силу ряд законов и постановлений правительства, связанных со стандартизацией и сертификацией продукции и услуг, в частности:

Закон Российской Федерации от 10 июня 1993 г. № 5151-1 "О сертификации продукции и услуг" с последующими изменениями и дополнениями;

Закон Российской Федерации от 10 июня 1993 г. № 5154-1 "О стандартизации".

Федеральный закон "О техническом регулировании" является системообразующим для построения принципиально новой системы сертификации и стандартизации, в которой бы учитывались демократические принципы нормативного регулирования, повышался бы уровень безопасности потребителей продукции и услуг, а также учитывались реалии рыночного устройства экономических отношений.

В настоящее время этот закон для интересующей нас области следует рассматривать вместе с **Федеральным законом от 1.05.2007 №65-ФЗ «О внесении изменений в ФЗ «О техническом регулировании».**

Основной упор в Федеральном законе «О техническом регулировании» делается на сужение сферы обязательной стандартизации и подтверждения соответствия и расширении добровольности таких действий. При этом подразумевается, что именно рыночная конъюнктура подтолкнет производителей осуществлять данную деятельность, чтобы обеспечить конкурентоспособность производимой продукции.

В законе даны определения ряда понятий.

*Аккредитация* – официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия.

*Знак соответствия* – обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту.

*Сертификация* – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

*Сертификат соответствия* – документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров.

*Стандарт* – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

*Стандартизация* – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышения конкурентоспособности продукции, работ или услуг.

*Техническое регулирование* – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнение работ или оказание услуг и правовое регулирование отношений в области оценки соответствия.

*Технический регламент* – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством, или федеральным законом, или указом Президента, или постановлением Правительства, и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации).

В качестве основных принципов технического регулирования в Законе приняты следующие:

независимость органов по аккредитации и сертификации от изготовителей, продавцов, исполнителей и приобретателей;

единая система и правила аккредитации;

единство правил и методов исследований (испытаний) и измерений при проведении процедур обязательной оценки соответствия;

единство применения требований технических регламентов независимо от видов или особенностей сделок;

недопустимость совмещения одним органом полномочий на аккредитацию и сертификацию и др.

В Законе предписано федеральным органам исполнительной власти издавать в сфере технического регулирования акты только рекомендательного характера, за исключением случаев, связанных с оборонной продукцией и продукцией, сведения о которой составляют государственную тайну.

Основное новшество в новом Законе – **технический регламент**, который устанавливает минимально необходимые требования, обеспечивающие безопасность в различных сферах, а также электромагнитную совместимость в части обеспечения безопасности работы приборов и оборудования, а также единство измерений.

В качестве основы технического регламента могут использоваться международные и/или национальные стандарты.

Технический регламент принимается федеральным законом или постановлением Правительства РФ и вступает в силу не ранее чем через 6 месяцев со дня его официального опубликования.

В России действуют общие и специальные технические регламенты. В качестве разработчика технического регламента может выступить любое лицо. Проект технического регламента должен быть опубликован в печатном издании или в информационной системе общего пользования. Федеральным органом исполнительной власти в области технического регулирования определено ***Федеральное агентство по техническому регулированию и метрологии***, входящее в Министерство промышленности и энергетики. Публичное обсуждение проекта технического регламента должно быть не менее 2-х месяцев. Подробно описан механизм прохождения закона о техническом регламенте в Госдуме и перечень необходимых документов. В исключительных случаях Президент России вправе издать технический регламент без его публичного обсуждения. До вступления в силу Федерального закона о техническом регламенте Правительство России вправе издать постановление о соответствующем регламенте.

Большое внимание в Законе уделено вопросам стандартизации. Определены цели и принципы стандартизации. Одним из принципов является ***добровольное* применение стандартов.**

К документам в области стандартизации, используемым на территории Российской Федерации, относятся:

национальные стандарты;

правила стандартизации, нормы и рекомендации в области стандартизации;

общероссийские классификаторы технико-экономической и социальной информации;

стандарты организаций.

Стандарты организаций, в том числе коммерческих, общественных, научных и саморегулируемых организаций, объединений юридических лиц могут разрабатываться в целях, не противоречащих настоящему закону. Проект стандарта может представляться в технический комитет по стандартизации, который проводит его экспертизу.

**Четвертая глава** закона посвящена подтверждению соответствия, означающему, что представляемая продукция, процессы и др. соответствует техническим регламентам, стандартам, условиям договоров. Подтверждение соответствия на территории РФ может носить добровольный или обязательный характер. Подробнее об этом будет сказано в 4 главе настоящего издания.

В **пятой главе** закона рассмотрены вопросы, связанные с аккредитацией органов по сертификации и испытательных лабораторий (центров).

Шестая глава посвящена государственному контролю (надзору) за соблюдением технических регламентов.

**Седьмая глава** посвящена ответственности за несоответствие продукции и др. требованиям технических регламентов и порядка отзыва продукции из обращения.

**Восьмая глава** "Информация о технических регламентах и документах по стандартизации" определяет порядок публикации информации о технических регламентах. Здесь также описано назначение Федерального информационного фонда технических регламентов и стандартов.

В заключительных положениях записано, что технические регламенты должны быть приняты в течение 7 лет со дня вступления в силу этого закона. Здесь также описан порядок работы до вступления в силу технических регламентов.

Реализация положений этого закона и контроль за их исполнением возложена на *Федеральное агентство по техническому регулированию и метрологии*. Положение о нем утверждено **постановлением Правительства от 17 июня 2004 г. № 294.**

Применительно к потребностям сферы защиты информации, законодательство о техническом регулировании необходимо было совершенствовать. Эта работа завершилась принятием **Федерального закона от 1.05.2007 №65-ФЗ «О внесении изменений в ФЗ «О техническом регулировании».**

**Федеральный закон от 29 июля 2004 г. № 98-ФЗ "О коммерческой тайне".**

Регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.

Данный закон вводит в правовые поле все принятые ранее документы федерального и регионального уровней, касающиеся коммерческой тайны, и конкретизирует положения статьи 139 Гражданского кодекса Российской Федерации "Служебная и коммерческая тайна".

Положения Закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

В Законе используются следующие основные понятия:

*Коммерческая тайна* – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

*Информация, составляющая коммерческую тайну* – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

*Режим коммерческой тайны* – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

*Обладатель информации*, составляющей коммерческую тайну – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайне.

*Доступ к информации*, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

*Разглашение информации*, составляющей коммерческую тайну – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, или иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

В Законе однозначно определен перечень сведений, которые не могут составлять коммерческую тайну:

1. Содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры.

2. Содержащиеся в документах, дающих право на осуществление предпринимательской деятельности.

3. О составе имущества государственного или муниципального унитарного предприятия и об использовании ими средств соответствующих бюджетов.

4. О загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом.

5. О численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест.

6. О задолженности работодателей по выплате заработной платы и по иным социальным выплатам.

7. О нарушении законодательства и фактах привлечения к ответственности за совершение этих нарушений.

8. Об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности.

9. О размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации.

10. О перечне лиц, имеющих право действовать без доверенности от имени юридического лица.

11. Обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Закон однозначно определяет круг лиц и организаций, кому необходимо представлять информацию, составляющую коммерческую тайну.

Такую информацию по мотивированному требованию необходимо предоставлять органу государственной власти, иного государственного органа, органа местного самоуправления. Информация предоставляется безвозмездно. Само мотивированное требование должно быть подписано уполномоченным лицом и содержать указание цели и правового основания затребования информации, срок предоставления информации. Если обладатель информации, составляющей коммерческую тайну, отказывается ее предоставлять, то соответствующие органы вправе потребовать ее предоставление по суду.

На всех документах, предоставляемых по требованию соответствующих органов, должен быть нанесен **гриф "коммерческая тайна"** с указанием ее обладателя (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество и место жительства).

Закон определяет права обладателя информации, обладающей коммерческой тайной, по установлению режима коммерческой тайны, его изменения, порядка использования, организации доступа, охраны информации, составляющей коммерческую тайну.

Обладатель информации, имеющей гриф "коммерческая тайна", должен принимать меры по ее охране. Эти меры должны включать:

перечень информации, составляющей коммерческую тайну;

установление порядка доступа и порядка обращения с такой информацией, а также способы контроля за установленным порядком;

учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была представлена или передана;

регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "коммерческая тайна" с указанием обладателя этой информации.

Кроме этих мер обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие, не противоречащие законодательству меры.

Для осуществления принимаемых мер работодатель обязан:

ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения своих обязанностей, с перечнем такой информации;

ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушения;

создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

Работник обязан не разглашать информацию, составляющую коммерческую тайну не только в период работы, но и после прекращения действия трудового договора в течение срока, предусмотренного соглашением между ними или в течение **3-х лет** после прекращения трудового договора, если указное соглашение не заключалось.

При разглашении информации, составляющей коммерческую тайну, работник обязан возместить нанесенный ущерб.

При увольнении, работник обязан передать работодателю все имеющиеся в его распоряжении материальные носители с информацией, содержащей коммерческую тайну.

Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства о коммерческой тайне. Размер убытков определяется в соответствие с гражданским законодательством.

Органы власти всех уровней обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями. При нарушении режима конфиденциальности работники органов власти несут ответственность в соответствии с законодательством.

**Закон Российской Федерации от 21 июля 1993 г. № 5485-1 "О государственной тайне" (с изменениями и дополнениями).**

Определяет основные понятия, полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты. Дает перечень сведений, которые могут быть отнесены к государственной тайне. Указывает принципы засекречивания сведений, перечисляет сведения, не подлежащие засекречиванию, устанавливает степени секретности сведений и грифы секретности носителей этих сведений. Описывает порядок отнесения сведений к государственной тайне, порядок рассекречивания сведений.

Правовой институт государственной тайны самый разработанный из числа правовых систем ограничения в доступе к информации. Однако развитие компьютерных систем создало для традиционной системы обеспечения режима секретности, в основном ориентированной на оборот документированной информации на бумажных носителях, много проблем.

Положения Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной властей, местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне (**статья 1**).

В Законе используются следующие основные понятия:

***государственная тайна*** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

***носители сведений*,** составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

***система защиты государственной тайны*** – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

*допуск к государственной тайне* – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений;

***доступ к сведениям***, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

***гриф секретности*** – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

***средства защиты информации*** – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

***перечень сведений****,* ***составляющих государственную тайну****,* –совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации О безопасности и включает настоящий Закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны (**статья 3**).

В Законе определяются и законодательно закрепляются полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты (статья 4), а также задается в общем виде перечень сведений, которые могут быть отнесены к государственной тайне (**статья 5** ).

***Засекречивание сведений и их носителей*** – введение в предусмотренном Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям. Засекречивание сведений осуществляется в соответствии с принципами законности, обоснованности и своевременности.

***Законность засекречивания сведений*** заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 Закона и законодательству Российской Федерации о государственной тайне.

***Обоснованность засекречивания сведений* заключается в установлении путем *экспертной оценки*** целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта, исходя из баланса жизненно важных интересов государства, общества и граждан.

*Своевременность засекречивания сведений* заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым **Распоряжением Президента России от 17 января 2000 г. № 6-рп.** Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Закон определяет сведения, не подлежащие засекречиванию (**статья 7**):

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах Российской Федерации;

о состоянии здоровья высших должностных лиц Российской Федерации;

о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

Должностные лица, наделенные полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан, если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению. При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну в соответствии с действующим законодательством.

Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника информации, его права. Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации.

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих работ. При этом до передачи сведений, составляющих государственную тайну, заказчик обязан убедиться в наличии у предприятия, учреждения или организации лицензии на проведение работ с использованием сведений соответствующей степени секретности, а у граждан – соответствующего допуска.

Предприятия, учреждения или организации, в том числе и негосударственных форм собственности, при проведении совместных и других работ (получении государственных заказов) и возникновении в связи с этим необходимости в использовании сведений, составляющих государственную тайну, могут заключать с государственными предприятиями, учреждениями или организациями договоры об использовании услуг их структурных подразделений по защите государственной тайны, о чем делается соответствующая отметка в лицензиях на проведение работ с использованием сведений, составляющих государственную тайну, обеих договаривающихся сторон.

В Законе устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: *особой важности, совершенно секретно и секретно*. Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

**Статья 12** Закона определяет реквизиты носителей сведений, составляющих государственную тайну. На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

о регистрационном номере;

о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, они указываются в сопроводительной документации на этот носитель.

**Статья 20 раздела VI** Закона относит к органам, осуществляющим защиту государственной тайны на территории Российской Федерации, следующие органы:

межведомственную комиссию по защите государственной тайны;

федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы;

органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством Российской Федерации.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

согласие на частичные, временные ограничения их прав в соответствии со статьей 24 настоящего Закона (право выезда за рубеж, право неприкосновенности частной жизни, право на распространение сведений об открытиях и изобретениях);

письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

определение видов, размеров и порядка предоставления льгот, предусмотренных настоящим Законом;

ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо.

Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий.

Закон (**статья 27**) определяет порядок допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, и порядок сертификации средств защиты информации (**статья 28**).

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

наличие у них сертифицированных средств защиты информации.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации.

Координация работ по организации сертификации средств защиты информации возлагается на Межведомственную комиссию по защите государственной тайны. Положение об этой комиссии и ее состав утверждены Указом Президента Российской Федерации от 6.10.2004 г. № 1286.

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях осуществляют федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности (Федеральная служба безопасности Российской Федерации), федеральный орган исполнительной власти, уполномоченный в области обороны (Министерство оброны Российской Федерации), федеральный орган исполнительной власти, уполномоченный в области внешней разведки (Служба внешней разведки Российской Федерации), федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), и их территориальные органы, на которые эта функция возложена законодательством Российской Федерации.

**Федеральный закон от 7 июля 2003 г. № 126-ФЗ "О связи" (с изменениями и дополнениями).**

Устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

**Статья 63** Закона устанавливает понятие **тайны связи**:

На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

Операторы связи обязаны обеспечить соблюдение тайны связи.

**Закон Российской Федерации от 27 ноября 1992 г. № 4015-1 "Об организации страхового дела в Российской Федерации" (с изменениями и дополнениями).**

Регулирует отношения между лицами, осуществляющими виды деятельности в сфере страхового дела, или с их участием, отношения по осуществлению государственного надзора за деятельностью субъектов страхового дела, а также иные отношения, связанные с организацией страхового дела.

**Статья 33** Закона предписывает соблюдение коммерческой и иной охраняемой законом тайны субъекта страхового дела должностными лицами органа страхового надзора, за исключением случаев, предусмотренных законодательством Российской Федерации.

**Федеральный закон от 3 февраля 1996 г. № 17-ФЗ "О внесении изменений и дополнений в Закон РСФСР от 2 декабря 1990 г. № 395‑1 "О банках и банковской деятельности в РСФСР" (с изменениями и дополнениями).**

Регулирует деятельность банковской системы Российской Федерации, которая включает в себя Банк России, кредитные организации, а также филиалы и представительства иностранных банков.

**Статья 26** Закона определяет понятие **банковской тайны**:

Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, налоговым органам, таможенным органам Российской Федерации в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора – органам предварительного следствия по делам, находящимся в их производстве.

**Федеральный закон от 7 августа 2001 г. № 119-ФЗ "Об аудиторской деятельности" (с изменениями и дополнениями).**

Определяет правовые основы регулирования аудиторской деятельности в Российской Федерации.

**Статья 8** Закона определяет понятие **аудиторской тайны**:

Аудиторские организации и индивидуальные аудиторы обязаны хранить тайну об операциях аудируемых лиц и лиц, которым оказывались сопутствующие аудиту услуги.

Аудиторские организации и индивидуальные аудиторы обязаны обеспечивать сохранность сведений и документов, получаемых и (или) составляемых ими при осуществлении аудиторской деятельности, и не вправе передавать указанные сведения и документы или их копии третьим лицам либо разглашать их без письменного согласия организаций и (или) индивидуальных предпринимателей, в отношении которых осуществлялся аудит и оказывались сопутствующие аудиту услуги, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами.

Федеральный орган исполнительной власти, осуществляющий государственное регулирование аудиторской деятельности, и иные лица, получившие доступ к сведениям, составляющим аудиторскую тайну в соответствии с настоящим Федеральным законом и другими федеральными законами, обязаны сохранять конфиденциальность в отношении таких сведений.

**Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 "О средствах массовой информации" (с изменениями и дополнениями).**

Устанавливает правовую основу деятельности в области массовой информации, включая термины и определения, принципы, организационные основы и ограничения в распространении информации.

**Федеральный закон от 18 июля 1995 г. № 108-ФЗ "О рекламе" (с изменениями и дополнениями).**

Регулирует отношения, возникающие в процессе производства, размещения и распространения рекламы на рынках товаров, работ, услуг Российской Федерации, включая рынки банковских, страховых и иных услуг, связанных с пользованием денежными средствами граждан (физических лиц) и юридических лиц, а также рынки ценных бумаг.

**Статья 27** Закона определяет право доступа к любой информации сотрудников антимонопольных органов и обязует их хранить коммерческую тайну, а также иметь при необходимости допуск к государственной тайне.

**Закон Российской Федерации от 5 марта 1992 г. № 2446-1 "О безопасности" (с изменениями и дополнениями).**

Закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

**Федеральный закон от 3 апреля 1995 г. № 40-ФЗ "Об органах федеральной службы безопасности в Российской Федерации" (с изменениями и дополнениями).**

Определяет назначение, правовые основы, принципы, направления деятельности, полномочия, силы и средства органов федеральной службы безопасности, а также порядок контроля и надзора за их деятельностью.

**Статья 7** Закона определяет защиту сведений о федеральной службе безопасности:

1. Граждане Российской Федерации, принимаемые на военную службу (работу) в органы федеральной службы безопасности, а также допускаемые к сведениям об органах федеральной службы безопасности, проходят процедуру оформления допуска к сведениям, составляющим государственную тайну, если иной порядок не предусмотрен законодательством Российской Федерации. Такая процедура включает в себя принятие обязательства о неразглашении указанных сведений.

2. В случаях, предусмотренных федеральными законами и иными нормативными правовыми актами Российской Федерации, указанный порядок распространяется на граждан Российской Федерации, принимаемых на военную службу (работу) в пограничные войска, а также допускаемых к сведениям о пограничных войсках.

Кроме того, **статьи 17 и 19** Закона определяют:

1. Сведения о сотрудниках органов федеральной службы безопасности, выполнявших (выполняющих) специальные задания в специальных службах и организациях иностранных государств, в преступных группах, составляют государственную тайну и могут быть преданы гласности только с письменного согласия указанных сотрудников и в случаях, предусмотренных федеральными законами.

2. Сведения о лицах, оказывающих или оказывавших органам федеральной службы безопасности содействие на конфиденциальной основе, составляют государственную тайну и могут быть преданы гласности только с письменного согласия этих лиц и в случаях, предусмотренных федеральными законами.

**Федеральный закон от 12 августа 1995 г. № 144-ФЗ "Об оперативно-розыскной деятельности" (с изменениями и дополнениями).**

Определяет содержание оперативно-розыскной деятельности, осуществляемой на территории Российской Федерации, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий.

**Статья 12** Закона определяет защиту сведений об органах, осуществляющих оперативно-розыскную деятельность:

Сведения об используемых или использованных при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и о тактике проведения оперативно-розыскных мероприятий составляют *государственную тайну* и подлежат рассекречиванию только на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность.

**Федеральный закон от 25 июля 1998 г. № 130-ФЗ "О борьбе с терроризмом" (с изменениями и дополнениями).**

Определяет правовые и организационные основы борьбы с терроризмом в Российской Федерации, порядок координации деятельности осуществляющих борьбу с терроризмом федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, общественных объединений и организаций независимо от форм собственности, должностных лиц и отдельных граждан, а также права, обязанности и гарантии граждан в связи с осуществлением борьбы с терроризмом.

**Статья 15** Закона определяет порядок информирования общественности о ходе контртеррористической операции.

**Федеральный закон от 27 июля 2006 г. № 149-ФЗ. "Об информации, информационных технологиях и о защите информации"( вместо ФЗ от 20 февраля 1995 г. № 24-ФЗ. "Об информации, информатизации и защите информации" (с изменениями и дополнениями в соответствии с ФЗ от 10 января 2003 г. № 15-Ф3).)**

Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации.

Определяет условия для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защиту интересов России, ее субъектов и муниципальных объединений, а также физических и юридических лиц при международном информационном обмене.

Рассмотрим основные положения этого закона.

О части основных понятий, используемых в ФЗ уже говорилось. Это следующие понятия:

1) информация,

2) информационные технологии,

3) информационная система,

4) информационно-телекоммуникационная сеть,

5) обладатель информации,

6) доступ к информации,

7) конфиденциальность информации,

10) электронное сообщение,

11) документированная информация.

Они фактически являются основными понятиями всего курса. Приведем те, которые еще не рассматривались.

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

**Статья 5 п.2.** отмечает, что информация в зависимости от категории доступа к ней подразделяется на **общедоступную информацию**, а также на информацию, доступ к которой ограничен федеральными законами (**информация ограниченного доступа**).

Далее понятие общедоступной информации раскрывается в **статье 7.**

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Важно, что согласно **п.4 статьи 8** , не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

В **статье 9** излагаются ограничения доступа к информации.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим **коммерческую тайну** (№ 98-ФЗ от 29 июля 2004г. «О коммерческой тайне»), **служебную тайну** и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (**профессиональная тайна**), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей **личную или семейную тайну**, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами. Порядок доступа к **персональным данным** граждан (физических лиц) устанавливается федеральным законом «О персональных данных» (№ 152-ФЗ от 27 июля 2006 г. ).

**Статья 6** посвящена обладателю информации. Им может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование. Обладатель информации вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Далее в **статье 13 п.3** о информационных системах, говорится, что «права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных».

Важны и обязанности обладателя информации:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

**Статья 11** касается документированной информации.

Здесь важно отметить, что электронное сообщение, подписанное **электронной цифровой подписью** или **иным аналогом собственноручной подписи**, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

**Статья 12** о государственном регулировании в сфере применения ИТ гласит в частности, что оно предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации);

2) **развитие информационных систем** различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) **создание условий** для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "**Интернет**" и иных подобных информационно-телекоммуникационных сетей.

**Статья 13** об информационных системах (ИС) отмечает, что **оператором информационной системы** является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с **техническими регламентами**, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем. Порядок создания и эксплуатации информационных систем, **не являющихся государственными ИС или муниципальными ИС**, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

Непосредственно государственных ИС касается **статья 14**. Здесь важно отметить, что **технические средства**, предназначенные для обработки информации, содержащейся в государственных ИС, в том числе программно-технические средства и **средства защиты информации**, должны соответствовать требованиям законодательства Российской Федерации **о техническом регулировании**.

Наконец, статья 16. дает определение и посвящена защите информации.

**Защита информации** представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.

Важно, что обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Обращает на себя внимание **п. 6 статьи 16**., согласно которому, федеральными законами могут быть установлены **ограничения использования определенных средств защиты** информации и осуществления отдельных видов деятельности в области защиты информации.

В **статье 17** устанавливается ответственность (дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации) за правонарушения ИТ и защиты информации. Именно:

Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

Но при этом, требование о возмещении убытков **не может быть удовлетворено** в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации **не несет** лицо, оказывающее услуги:

1)либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

**Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ (действующая редакция, 2016).**

Обеспечивает правовые условия использования электронной цифровой подписи (ЭЦП) в электронных документах. Приведены основные понятия, используемые в электронных документах и условия использования ЭЦП.

**Закон Российской Федерации от 23 сентября 1992 г. № 3526-1 "О правовой охране топологий интегральных микросхем" (с изменениями и дополнениями).**

Регулирует отношения, связанные с созданием, правовой охраной и использованием топологий.

**Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ “О персональных данных”.**

Регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Важно, что он **не распространяется** на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда РФ и других архивных документов в соответствии с законодательством об архивном деле в РФ;

3) обработке подлежащих включению в **единый государственный реестр индивидуальных предпринимателей** сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством РФ в связи с деятельностью физического лица в качестве индивидуального предпринимателя;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

В законе используются следующие основные понятия:

1) **персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2) **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

3) **обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

4) **распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

5) **использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

6) **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

7) **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

8) **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

9) **информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

10) **конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

11) **трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

12) **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

К закону было подготовлено **Постановление Правительства РФ от 17 ноября 2007 г. N 781** «**Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных**». ФСБ и ФСТЭК России подготовили и другие документы.

**Положение** устанавливает **требования к обеспечению безопасности** персональных данных при их обработке в информационных системах (ИС) персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

Под **техническими средствами**, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Безопасность персональных данных** достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью **системы защиты персональных данных**, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Методы и способы защиты информации в информационных системах устанавливаются **Федеральной службой по техническому и экспортному контролю (ФСТЭК)** и **Федеральной службой безопасности (ФСБ)** Российской Федерации в пределах их полномочий. (Подготовлены в марте 2008года).

Безопасность персональных данных при их обработке в ИС обеспечивает **оператор** или **уполномоченное лицо**, которому на основании договора оператор поручает обработку персональных данных. Эти лица при обработке персональных данных в ИС должны обеспечить:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

**Мероприятия по обеспечению безопасности** персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

Важные разделы касаются разработчиков средств защиты информации, на которых возлагается реализация требований по обеспечению безопасности.

В отношении разработанных **шифровальных (криптографических) средств защиты** информации, проводятся тематические исследования и контрольные тематические исследования. При этом под **тематическими исследованиями** понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами информационных систем, а под **контрольными тематическими исследованиями** - периодически проводимые тематические исследования.

Результаты оценки соответствия и (или) тематических исследований средств защиты информации, оцениваются в ходе экспертизы, осуществляемой ФСТЭК и ФСБ Российской Федерации в пределах их полномочий.

**Основные подзаконные акты в области защиты информации**

Количество подзаконных актов федерального уровня и уровня субъектов федерации, изданных во исполнение рассмотренных выше законов, выпущено более сотни. Кроме того, в них постоянно вносятся изменения и уточнения. Ниже представлено краткое содержание только основных из таких подзаконных актов, определяющих либо основы деятельности в различных сферах, связанных с защитой информации, либо наиболее часто требующихся на практике. Все такие акты разделены на три категории: указы Президента Российской Федерации, Постановления Правительства Российской Федерации и ведомственные документы. Более подробно о них можно посмотреть в учебнике [Тихонов-Райх ].

Отметим, что в связи с проведением административной реформы в Российской Федерации названия соответствующих органов исполнительной власти, упоминающихся в рассматриваемых документах изменены на новые или на названия преемников ликвидированных ведомств (например, ФАПСИ – ликвидировано 11.03.2003г.), за исключением Гостехкомиссии (ныне Федеральной службы по техническому и экспортному контролю, ФСТЭК).

### Указы Президента Российской Федерации

**4.** Указ Президента Российской Федерации от 31 декабря 1993 г. № 2334 "**О дополнительных гарантиях прав граждан на информацию**" (с изменениями от 17 января 1997 г., 1 сентября 2000 г.).

Указ определяет, что деятельность государственных органов, организаций и предприятий, общественных объединений, должностных лиц должна осуществляться на следующих принципах информационной открытости:

доступность для граждан информации, представляющей общественный интерес или затрагивающей личные интересы граждан;

систематическое информирование граждан о предполагаемых или принятых решениях;

осуществление гражданами контроля за деятельностью государственных органов, организаций и предприятий, общественных объединений, должностных лиц и принимаемыми ими решениями, связанными с соблюдением, охраной и защитой прав и законных интересов граждан;

создание условий для обеспечения граждан Российской Федерации зарубежными информационными продуктами и оказание им информационных услуг, имеющих зарубежное происхождение.

Устанавливается, что в информационных программах государственных телерадиовещательных компаний до сведения граждан в обязательном порядке должны доводиться основные положения правовых актов и решений государственных органов по основными вопросам внутренней и внешней политики *в день их выпуска*. Государственные телерадиовещательные компании должны создать циклы передач (программы), разъясняющие деятельность федеральных органов законодательной, исполнительной и судебной власти, существо принимаемых решений с привлечением к работе над этими программами ведущих специалистов, экспертов, разработчиков соответствующих документов.

**5.** Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 "**О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации**" (с изменениями от 25 июля 2000 г.).

Указ определяет порядок использования шифровальных средств.

Запрещается использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата ФСБ России, а также размещение государственных заказов на предприятиях, в организациях, использующих указанные технические и шифровальные средства, не имеющие соответствующего сертификата.

Центральному банку России указывается принять необходимые меры в отношении коммерческих банков Российской Федерации, уклоняющихся от обязательного использования имеющих сертификат ФСБ России защищенных технических средств хранения, обработки и передачи информации при их информационном взаимодействии с подразделениями Центрального Банка России.

В интересах информационной безопасности Российской Федерации и усиления борьбы с организованной преступностью запрещается деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации, без лицензий, выданных ФСБ России.

Федеральной таможенной службе Российской Федерации указывается принять меры к недопущению ввоза на территорию Российской Федерации шифровальных средств иностранного производства без соответствующей лицензии Министерства торговли и экономического развития, выданной по согласованию с ФСБ России.

**9.** Указ Президента Российской Федерации от 9 января 1996 г. № 21 "**О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации**" (с изменениями от 30 декабря 2000 г.).

В соответствии с Федеральным законом "Об оперативно-розыскной деятельности" Указ возлагает на ФСБ России следующие обязанности:

лицензирование деятельности не уполномоченных на осуществление оперативно-розыскной деятельности физических и юридических лиц, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввозом в Российскую Федерацию и вывозом за ее пределы специальных технических средств, предназначенных для негласного получения информации, а также сертификацию, регистрацию и учет таких специальных технических средств;

выявление и пресечение случаев проведения оперативно-розыскных мероприятий и использования специальных и иных технических средств, разработанных, приспособленных, запрограммированных для негласного получения информации, неуполномоченными лицами;

координацию деятельности федеральных органов исполнительной власти, осуществляемой в соответствии с Федеральным законом "Об оперативно-розыскной деятельности", в области разработки, производства, закупки, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности.

*Положение* о лицензировании деятельности, связанной со специальными техническими средствами, предназначенными для негласного получения информации, утверждено Постановлением Правительства Российской Федерации от 15 июля 2002 г. № 526.

*Положение* о ввозе в Российскую Федерацию и вывозе из Российской Федерации указанных технических средств утверждено Постановлением Правительства Российской Федерации от 10 марта 2000 г. № 214.

*Перечень* видов специальных технических средств, предназначенных для негласного получения информации, утвержден Постановлением Правительства Российской Федерации от 1 июля 1996 г. № 770.

**14.** Указ Президента Российской Федерации от 15 февраля 2006 г. № 116 «**О мерах по противодействию терроризму**».

В соответствии с данным Указом образован Национальный антитеррористический Комитет. Председатель Комитета – директор ФСБ. Созданы антитеррористические комиссии в субъектах РФ. Увеличена численность Центрального аппарата ФСБ на 300 человек.

**15.** Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «**О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена**».

**Постановления Правительства Российской Федерации**

**1.** Постановление Правительства РФ от 15 апреля 1995 г. № 333 "**О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны**" (с изменениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г., 3 октября 2002 г.)

Данным Постановлением утверждено Положение о лицензировании деятельности, связанной с работой со сведениями, составляющими государственную тайну. В нем, в частности, сказано, что органами, уполномоченными на ведение лицензионной деятельности, являются:

по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, – Федеральная служба безопасности Российской Федерации и ее территориальные органы (на территории Российской Федерации), Служба внешней разведки Российской Федерации (за рубежом);

на право проведения работ, связанных с созданием средств защиты информации, – Государственная техническая комиссия при Президенте Российской Федерации (здесь и далее следует подразумевать новое название данной организации – ФСТЭК России), Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба безопасности Российской Федерации (в пределах их компетенции);

на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – Федеральная служба безопасности Российской Федерации и ее территориальные органы, Государственная техническая комиссия при Президенте Российской Федерации, Служба внешней разведки Российской Федерации (в пределах их компетенции).

Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, и при выполнении следующих условий:

соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;

наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее трех и более пяти лет.

Государственными органами, ответственными за организацию и проведение специальных экспертиз предприятий, являются Федеральная служба безопасности Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации, Служба внешней разведки Российской Федерации, другие министерства и ведомства Российской Федерации, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий.

**2.**Постановление Правительства РФ от 26 июня 1995 г. № 608 "**О сертификации средств защиты информации**" (с изменениями от 23 апреля 1996 г., 29 марта 2016 г.).

Данным Постановлением утверждено Положение о сертификации средств защиты информации, которое устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам.

Системы сертификации создаются Государственной технической комиссией при Президенте Российской Федерации, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, Службой внешней разведки Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации.

Сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции. Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны. В каждой системе сертификации разрабатываются и согласовываются с Межведомственной комиссией положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

Основными схемами проведения сертификации средств защиты информации являются:

для единичных образцов средств защиты информации – проведение испытаний этих образцов на соответствие требованиям по защите информации;

для серийного производства средств защиты информации – проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований. Кроме того, допускается предварительная проверка производства по специально разработанной программе.

Срок действия сертификата не может превышать пяти лет.

**11.** Постановление Правительства РФ от 10 марта 2000 г. № 214 "**Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию**" (с изменениями от 19 октября 2000 г.).

Контроль за ввозом в Российскую Федерацию и вывозом из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, не уполномоченными на осуществление оперативно-разыскной деятельности юридическими лицами обеспечивает Федеральная служба безопасности Российской Федерации и Федеральная таможенная служба Российской Федерации.

Лицензирование деятельности по ввоз указанные средств осуществляет Министерство экономического развития и торговли Российской Федерации на основании решений Центра Федеральной службы безопасности Российской Федерации по лицензированию, сертификации и защите государственной тайны.

**12.** Постановление Правительства РФ от 11 февраля 2002 г. № 135 "**О лицензировании отдельных видов деятельности**".

Устанавливает перечень федеральных органов исполнительной власти, осуществляющих лицензирование в определенных областях, а также виды деятельности, лицензируемые органами исполнительной власти субъектов Российской Федерации.

Защиты информации в данном Постановлении касается лицензирование следующих видов деятельности.

*МВД России*: негосударственная (частная) охранная деятельность, негосударственная (частная) сыскная деятельность;

*МЧС России*: производство работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений;

*ФСБ России*:

разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

деятельность по распространению шифровальных (криптографических) средств;

деятельность по техническому обслуживанию шифровальных (криптографических) средств;

предоставление услуг в области шифрования информации;

разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

*ФСТЭК России*:

деятельность по технической защите конфиденциальной информации;

деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

**13.** Постановление Правительства РФ от 30 апреля 2002 г. № 290 "**О лицензировании деятельности по технической защите конфиденциальной информации**".

Положение определяет порядок лицензирования деятельности юридических и физических лиц по технической защите конфиденциальной информации.

Под *технической защитой конфиденциальной информации* понимается комплекс мероприятий и (или) услуг по защите ее от НСД, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней.

Право выдачи лицензий имеет ФСТЭК России.

Лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

а) осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности "компьютерная безопасность", "комплексное обеспечение информационной безопасности автоматизированных систем" или "информационная безопасность телекоммуникационных систем", либо специалистами, прошедшими переподготовку по вопросам защиты информации;

б) соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами Российской Федерации и нормативно-методическими документами по технической защите информации;

в) использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;

г) использование третьими лицами программ для электронно-вычислительных машин или баз данных на основании договора с их правообладателем.

Положение также определяет перечень необходимых документов для получения лицензии и порядок ее выдачи. Срок действия лицензии установлен в 5 лет, потом она должна переоформляться. Один раз в год производится проверка выполнения лицензионных требований.

**14.** Постановление Правительства РФ от 27 мая 2002 г. № 348 "**Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации**".

Это Положение определяет порядок лицензирования деятельности юридических и физических лиц по разработке и (или) производству средств защиты конфиденциальной информации.

Лицензирование осуществляет ФСТЭК России, а в части разработки средств защиты для объектов Администрации Президента РФ, Совбеза РФ, Федерального Собрания РФ, Правительства РФ, Конституционного, Верховного и Высшего Арбитражного судов – ФСБ России.

Разрабатываемые устройства должны удовлетворять требованиям госстандартов РФ, соответствующей документации и иных нормативных актов, а также по уровню подготовки специалистов и выдерживать соответствие помещений и оборудования требованиям по защите информации. Для деятельности, лицензируемой ФСБ России в данной сфере набор лицензионных требований значительно шире.

Перечень необходимых документов для получения лицензии, порядок ее выдачи, срок действия лицензии и контроль за ее выполнением установлены Положением практически аналогично Постановлению № 290, рассмотренному выше.

**16.** Постановление Правительства РФ от 23 сентября 2002 г. № 691 "**Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами**".

Данным документом утверждаются 4 положения, касающиеся лицензирования отдельных видов деятельности в области криптографических средств:

1. Положение о лицензировании деятельности *по распространению* шифровальных (криптографических) средств.

2. Положение о лицензировании деятельности *по техническому обслуживанию* шифровальных (криптографических) средств.

3. Положение о лицензировании *предоставления услуг* в области шифрования информации.

4. Положение о лицензировании *разработки, производства* шифровальных (криптографических) средств защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

В перечисленных положениях дан перечень средств шифрования, имитозащиты, электронной цифровой подписи, кодирования, изготовления ключей и ключевых документов. При этом указано, что *не требуется* лицензирование для криптографических средств, осуществляющих преобразование информации с длиной ключа до 40 бит при использовании симметричного алгоритма и 128 бит – при использовании асимметричного алгоритма.

В качестве лицензирующего органа выступает ФСБ России. Здесь также определены лицензионные требования, а также перечень необходимых документов, представляемых в лицензионный орган и порядок рассмотрения и выдачи лицензии.

**19.** Постановление Правительства РФ от 30 мая 2003 г. № 313 "**Об уполномоченном федеральном органе исполнительной власти в области использования электронной цифровой подписи**".

В соответствии с Федеральным законом "Об электронной цифровой подписи" функции уполномоченного федерального органа исполнительной власти в области использования электронной цифровой подписи возлагаются на Министерство информационных технологий и связи Российской Федерации. При этом его деятельность в области использования ЭЦП в органах государственной власти России должна согласовываться с ФСБ России.

### Ведомственная нормативная база

***Нормативные документы и инструктивные материалы МВД РФ:***

Приказ МВД РФ от 22 августа 1992 г. № 292 "Об организации исполнения органами внутренних дел Закона Российской Федерации "О частной детективной и охранной деятельности в Российской Федерации" (с изменениями от 14 ноября 1994 г.).

Приказ МВД РФ от 31 декабря 1999 г. № 1105 "О мерах по усилению контроля органами внутренних дел за частной детективной и охранной деятельностью".

РД-78.143-92 "Системы и комплексы охранной сигнализации, элементы технической укрепленности объектов. Нормы проектирования".

РД-78.147-93 "Единые требования по технической укрепленности и оборудованию сигнализации охраняемых объектов".

***Нормативные документы и инструктивные материалы ФСБ РФ:***

1. Приказ ФСБ РФ от 13 ноября 1999 г. № 564 "Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия".

2. Приказ ФСБ РФ от 9 февраля 2005 г. № 66. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005).

Данное положение распространяется на СКЗИ, предназначенные для защиты информации с ограниченным доступом, но не содержащей сведения, составляющие государственную тайну.

3. Приказ ФАПСИ от 13 июня 2001 г. № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".

***Нормативные документы и инструктивные материалы ФСТЭК (Гостехкомиссии) РФ:***

1. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации». Руководящий документ Гостехкомиссии России,

2. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Руководящий документ Гостехкомиссии России,

***3.*** «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Руководящий документ Гостехкомиссии России,

***4.*** «Защита информации. Специальные защитные знаки. Классификация и общие требования». Руководящий документ Гостехкомиссии России,

***5.*** «Защита от несанкционированного доступа к информации. Термины и определения». Руководящий документ Гостехкомиссии России,

***6.*** «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Руководящий документ Гостехкомиссии России,

***7.*** Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1. Часть 2. Часть 3. Руководящий документ Гостехкомиссии России,

***8.*** «Инструкция о порядке проведения специальных экспертиз предприятий, учреждений и организаций на право осуществления мероприятий и (или) оказания услуг в области противодействия иностранной технической разведке». Утверждена Председателем Гостехкомиссии 17 октября 1995 г.

***9.*** «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России,

***10.*** Решение Гостехкомиссии от 3 октября 1995 г. № 42 «О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте»,

***11.*** Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Председателем Гостехкомиссии России 25 ноября 1994 г.

***12.*** Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации. Утверждено Председателем Гостехкомиссии России 25 ноября 1994 г.

***13.*** Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3,

***14.*** Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3,

***15.*** Типовое положение об испытательной лаборатории. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3,

***16.***  «Перечень средств защиты информации, подлежащих сертификации в системе сертификации Гостехкомиссии России» (N РОСС RU.0001.01БИ00);

***17.*** «Положение о государственном лицензировании деятельности в области защиты информации». Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительствен­ной связи и информации при Президенте Российской Федерации от 27.04.1994г. №10;

***18.*** «Положение о сертификации средств защиты информации по требованиям безопасности информации». Введено в действие Приказом Председателя Гостехкомиссии России от 27.10.1995г. №199;

***19.*** «Положение по аттестации объектов информатизации по требованиям безопасности информации». Утверждено Председателем Гостехкомиссии при Президенте Российской Федерации 25 ноября 1994 г.,

***20.*** «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР-97)» от 23 мая 1997 г. № 55,

***21.*** «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России,

***22.*** «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России.

***23.*** «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации». Руководящий документ Гостехкомиссии России;

***24.*** Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР — К)»,

***25.*** Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам. Руководящий документ Гостехкомиссии России,

***26.*** «Положение о государственном лицензировании деятельности в области защиты информации». Утверждено решением Гостехкомиссии при Президенте Российской Федерации и ФАПСИ при Президенте Российской Федерации от 24 апреля 1994 г. № 10 (в редакции решения от 24 июня 1997 г. № 60);

**Стандарты информационной безопасности**

В настоящее время все вопросы, связанные со стандартизацией в Российской Федерации, регулируются Федеральным законом "**О техническом регулировании**".

**Статья 11** Закона определяет цели стандартизации:

повышение уровня безопасности жизни или здоровья граждан, имущества, экологической безопасности, безопасности жизни или здоровья животных и растений;

повышение уровня безопасности объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера;

обеспечение научно-технического прогресса;

повышение конкурентоспособности продукции, работ, услуг;

рациональное использование ресурсов;

техническая и информационная совместимость;

сопоставимость результатов исследований (испытаний) и измерений, технических и экономико-статистических данных;

взаимозаменяемость продукции.

**Статья 13** Закона определяет виды документов в области стандартизации, к ним отнесены:

национальные стандарты;

правила стандартизации, нормы и рекомендации в области стандартизации;

применяемые в установленном порядке классификации, общероссийские классификаторы технико-экономической и социальной информации;

стандарты организаций.

**Статья 14** Закона определяет статус национального органа Российской Федерации по стандартизации и технических комитетов по стандартизации. В соответствии с данной статьей на указанный орган возложено выполнение следующих задач:

утверждение национальных стандартов;

принятие программы разработки национальных стандартов;

организация экспертизы проектов национальных стандартов;

обеспечение соответствия национальной системы стандартизации интересам национальной экономики, состоянию материально-технической базы и научно-техническому прогрессу;

осуществление учета национальных стандартов, правил стандартизации, норм и рекомендаций в этой области и обеспечение их доступности заинтересованным лицам;

создание технических комитетов по стандартизации и координация их деятельности;

организация опубликования национальных стандартов и их распространения;

участие в соответствии с уставами международных организаций в разработке международных стандартов и обеспечение учета интересов Российской Федерации при их принятии;

утверждение изображения знака соответствия национальным стандартам;

представительство Российской Федерации в международных организациях, осуществляющих деятельность в области стандартизации.

Орган, уполномоченный на исполнение функций национального органа по стандартизации, определяет Правительство Российской Федерации.

В соответствии с постановлениями Правительства РФ от 16 июня 2004 г. № 284 и от 17 июня 2004 г. № 294 функции федерального органа по техническому регулированию и национального органа по стандартизации осуществляет **Федеральное агентство по техническому регулированию и метрологии**. (Ростехрегулирование, ФАТР и М).

Официальным изданием является "Вестник технического регулирования", зарегистрированный под номером ПИ № 77-16464 от 22 сентября 2003 г.

Так, постановлением Госстандарта РФ от 30 января 2004 г. № 4 определено, что *национальными стандартами* Российской Федерации признаются государственные и межгосударственные стандарты, принятые Госстандартом России до 1 июля 2003 года.

Однако до вступления в силу соответствующих технических регламентов требования к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, установленные указанными национальными стандартами, подлежат обязательному исполнению *только в части*, соответствующей целям:

защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;

охраны окружающей среды, жизни или здоровья животных и растений;

предупреждения действий, вводящих в заблуждение приобретателей.

*Основополагающим государственным стандартом Российской Федерации в области защиты информации* является ГОСТ Р 52069.0-2003 "Защита информации. Система стандартов. Основные положения" (принят постановлением Госстандарта РФ от 5 июня 2003 г. № 181-ст).

Он устанавливает цель и задачи системы стандартов по защите информации, объекты стандартизации, структуру, состав и классификацию входящих в нее стандартов и правила их обозначения. Положения данного стандарта являются рекомендуемыми при разработке нормативных документов по стандартизации в области защиты информации, независимо от организационно-правовой формы и формы собственности предприятия, учреждения, организации – разработчика стандарта, а также при организации работ по стандартизации в области защиты информации органами управления Российской Федерации.

В соответствии с данным стандартом система стандартов по защите информации (ССЗИ) может включать в себя следующие нормативные документы:

регламенты;

стандарты;

правила, нормы и рекомендации по стандартизации;

общероссийские классификаторы технико-экономической информации;

нормативно-технические документы (НТД) системы общих технических требований к вооружению и военной технике (ОТТ).

В зависимости от объекта стандартизации в области ЗИ и требований, предъявляемых к нему, устанавливают стандарты следующих видов:

основополагающие;

на продукцию;

на процессы;

на технологию, включая в том числе информационные технологии;

на услуги;

на методы контроля;

на документацию;

на термины и определения.

**Стандарты по ЗИ подразделяют на следующие категории:**

международные (ГОСТ ИСО);

межгосударственные (ГОСТ);

государственные стандарты Российской Федерации, оформленные на основе аутентичного текста международного стандарта (ГОСТ Р ИСО/МЭК);

государственные стандарты Российской Федерации (ГОСТ Р);

государственные военные стандарты Российской Федерации (ГОСТ РВ);

стандарты отраслей, в том числе и на оборонную продукцию (ОСТ);

стандарты предприятий.

**В приложении дан** перечень основных стандартов, имеющих отношение к защите информации.

**Зарубежные стандарты в области информационной безопасности**

Стандарты и спецификации можно условно разделить на два вида:

* оценочные стандарты, направленные на классификацию информационных систем и средств защиты по требованиям безопасности;
* технические спецификации, регламентирующие различные аспекты реализации средств защиты.

Важно отметить, что между эти видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Технические спецификации имеют ряд положительных и отрицательных аспектов. Главные достоинства этих стандартов состоят в следующем:

Стандарт гарантирует большой сектор рынка для определенного типа оборудования или программного обеспечения. Это поощряет массовое производство и в некоторых случаях использование методов интеграции высокого и сверхвысокого уровня, что приводит к снижению цен.

Стандарт обеспечивает взаимодействие устройств, разработанных различными производителями, что обеспечивает большую гибкость при выборе и использовании оборудования.

Ниже перечислены основные недостатки технических стандартов:

Стандартизация ведет к замораживанию технологии. За то время пока стандарт разрабатывается, проходит проверку, согласуется, пересматривается и, наконец, публикуется, могут появиться новые, более эффективные технологии.

Существует множество стандартов, относящихся к одной и той же области деятельности. Это не является недостатком самих стандартов, а отражает сегодняшнюю технологию стандартизации. К счастью, в последние годы многие организации, занимающиеся разработкой стандартов, начали тесно сотрудничать. Тем не менее, существуют сферы, в которых стандарты иногда конфликтуют друг с другом.

**Стандарты и регулирование**

Следует различать следующие три понятия:

добровольные стандарты;

регулирующие стандарты;

регулятивное использование добровольных стандартов.

**Добровольные стандарты** разрабатываются организациями, производящими стандарты. Они являются добровольными в том смысле, что их существование не делает обязательным их применение. То есть, производители добровольно создают продукт, соответствующий стандарту, если они видят в этом выгоду для самих себя. Никаких юридических обязательств в этом нет. Эти стандарты также являются добровольными в том смысле, что они были разработаны добровольцами, предпринимаемые усилия которых не оплачивались организацией, производящей стандарты и управляющей этим процессом. Эти добровольцы являются служащими заинтересованных организаций, например производителей и государственных организаций. Работоспособность добровольных стандартов объясняется тем, что, как правило, эти стандарты разрабатывались на основе широкого консенсуса и что потребительский спрос на стандартизированные продукты поощрял применение этих стандартов производителями.

**Регулирующие стандарты**, напротив, разрабатываются государственными регулятивными управлениями для достижения определенной общественной цели, например в области безопасности. Эти стандарты обладают регулятивной силой и должны выполняться производителями в контексте применения данных предписаний. Но предписания могут применяться к широкому спектру продуктов, включая компьютеры и средства связи.

**Регулятивное использование добровольных стандартов** — относительно новое или, по меньшей мере, недавно ставшее превалирующим явление. Типичный пример этого — предписание, требующее от государственных организаций, чтобы они приобретали только продукт, соответствующий некоторому набору добровольных стандартов. У такого подхода есть ряд достоинств:

Он уменьшает бремя производства стандартов, лежащее на государственных организациях.

Он поощряет сотрудничество между государством и организациями по стандартизации в области производства стандартов широкого применения.

Он уменьшает число стандартов, которые должны выполнять производители.

Исторически первым широко распространившимся документом, получившем статус стандарта, были ***Критерии безопасности компьютерных систем*** Министерства обороны США.

Впоследствии они были приняты другими ведомствами этой страны и даже другими государствами либо в исходном виде, либо после переработки с учетом развития информационных технологий. Так появились *Европейские, Федеральные, Канадские* критерии безопасности компьютерных систем. В настоящее время в большинстве стран, в том числе и в России, силу стандарта приобрели так называемые *Общие критерии*.

Интересно посмотреть на краткое содержание предыдущих разработок, чтобы показать эволюцию научно-технической мысли в сфере стандартизации вопросов обеспечения информационной безопасности в ее узком, компьютерном понимании.

### Критерии безопасности компьютерных систем Министерства обороны США – "Оранжевая книга"

Критерии безопасности компьютерных систем (TCSEC – Trusted Computer System Evaluation Criteria), получившие неформальное, но прочно закрепившееся название "**Оранжевая книга**" (по цвету изданной брошюры), были разработаны Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем и выработки соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения.

В 1985 г. "Оранжевая книга" была принята в качестве стандарта Министерства обороны США (DoD TCSEC). В 1987 и 1991 гг. стандарт был дополнен требованиями для гарантированной поддержки политики безопасности в распределённых вычислительных сетях и базах данных.

В данном документе впервые нормативно определены такие понятия, как "**политика безопасности**", вычислительная база защиты или **ядро защиты** (ТCB, Trusted Computing Base) и т.д.

Согласно "Оранжевой книге", *безопасная компьютерная система* – это система, поддерживающая управление доступом к обрабатываемой в ней информации таким образом, что только соответствующим образом авторизованные пользователи или процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию. Предложенные в этом документе концепции защиты и набор функциональных требований послужили *основой для формирования всех появившихся впоследствии стандартов безопасности*.

В "Оранжевой книге" предложены три категории требований безопасности – политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних – на качество самих средств защиты. Рассмотрим эти требования подробнее.

*Требование 1.* Политика безопасности. Система должна поддерживать точно определенную политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основании их идентификации и набора правил управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации.

*Требование 2.* Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности объекта и/или режимы доступа к этому объекту.

*Требование 3.* Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификация) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения. Они должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

*Требование 4.* Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность. Это необходимо для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

*Требование 5.* Контроль корректности функционирования средств защиты. Средства защиты должны содержать независимые аппаратные функции защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

*Требование 6.* Непрерывность защиты. Все средства защиты (в т.ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

Приведенные выше базовые требования к безопасности служат основой для критериев, образующих *единую шкалу оценки безопасности компьютерных систем, определяющую семь классов безопасности*.

Все системы в соответствии с "Оранжевой книгой" распределяются по следующим **классам** **защищенности** (в порядке возрастания защищенности, более защищенный класс включает в себя все требования предыдущих классов):

Класс D – минимальная защита. Зарезервирован для отнесения систем, не удовлетворяющих ни одному из других классов защиты.

Класс С1 – защита, основанная на разграничении доступа (DAC). Обеспечивается разграничение пользователей и данных.

Класс С2 – защита, основанная на управляемом контроле доступом. Наличие усовершенствованных средств управления доступом и распространения прав, аудит событий, имеющих отношение к безопасности системы и разделению ресурсов. Общие ресурсы должны очищаться перед повторным использование другими процессами.

Класс В1 – мандатная защита, основанная на присваивании меток объектам и субъектам, находящимся под контролем ТСВ. Необходима реализация механизма присваивания меток экспортируемым данным.

Класс В2 – структурированная защита. Управление доступом распространяется на все субъекты и объекты системы. Анализ побочных каналов утечки информации. Специальные процедуры изменения конфигурации. Возможность тестирования и полного анализа ТСВ. Разбиение ее структуры на критические с точки зрения защиты и некритические элементы.

Класс В3 – домены безопасности. Реализация концепции монитора обращений, который гарантированно защищен от несанкционированного доступа, порчи и подделки, обрабатывает все обращения, прост для анализа и тестирования (предоставляется полная система тестов, полнота которой доказана).

Класс А1 – верифицированный проект. Проект ТСВ должен быть представлен в виде формализованной и верифицированной математическими методами спецификации.

Выбор класса защиты системы рекомендуется осуществлять на основе ее **режима функционирования**. Определяется пять таких режимов:

1. Режим, в котором система постоянно обрабатывает ценную информацию одного класса в окружении, которое обеспечивает безопасность для работы с этим классом.

2. Режим особой секретности самой системы. Все пользователи и элементы системы имеют один класс и могут получить доступ к любой информации.

3. Многоуровневый режим. Обработка информации разных классов, не все пользователи имеют доступ ко всем классам информации.

4. Контролирующий режим. Многоуровневый режим, в котором защищенность ТСВ полностью не гарантируется.

5. Режим изолированной безопасности. Изолированная обработка информации различных классов. Например, защищаться может лишь один класс информации, а остальные нет.

Основой для выбора класса является **индекс риска**: разность между максимальным классом (грифом) информации и минимальным классом пользователей. Чем выше разность, тем больший класс защиты требуется.

Следует отметить, что "Критерии безопасности компьютерных систем" Министерства обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на разработчиков, потребителей и специалистов по сертификации компьютерных систем.

Основной отличительной чертой этого документа является его ориентация на системы военного применения, причем в основном на *операционные системы*. Это предопределило доминирование требований, направленных на обеспечение конфиденциальности обрабатываемой информации и исключение возможностей ее разглашения.

Критерии адекватности реализации средств защиты и политики безопасности отражены слабо, соответствующий раздел по существу ограничивается требованиями контроля целостности средств защиты и поддержания их работоспособности, что явно недостаточно.

### Европейские критерии безопасности информационных технологий

Проблемы стандартизации в сфере информационной безопасности оказались актуальны не только для Соединенных штатов. Вслед за выходом "Оранжевой книги" страны Европы разработали согласованные "**Критерии безопасности информационных технологий**" (Information Technology Security Evaluation Criteria, далее – Европейские критерии). Европейские критерии рассматривают следующие задачи средств информационной безопасности:

защита информации от несанкционированного доступа с целью обеспечения ее *конфиденциальности*;

обеспечение *целостности* информации посредством защиты от ее несанкционированной модификации или уничтожения;

обеспечение *доступности* компьютерных систем с помощью противодействия угрозам отказа в обслуживании.

Для того, чтобы удовлетворить требованиям конфиденциальности, целостности и доступности, необходимо реализовать соответствующий набор функций безопасности, таких как идентификация и аутентификация, управление доступом, восстановление после сбоев и т.д. Чтобы средства защиты можно было признать эффективными, требуется определенная степень уверенности в правильности их выбора и надежности функционирования. Для решения этой проблемы в Европейских критериях впервые вводится понятие ***адекватности* (assurance) средств защиты**.

Адекватность включает в себя два аспекта: *эффективность*, отражающую соответствие средств безопасности решаемым задачам, и *корректность*, характеризующую процесс их разработки и функционирования.

Эффективность определяется соответствием между задачами, поставленными перед средствами безопасности, и реализованным набором функций защиты – их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты. Под корректностью понимается правильность и надежность реализации функций безопасности.

Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

Главное достижение этого документа – введение понятия адекватности средств защиты и определение отдельной шкалы для критериев адекватности.

Необходимо отметить, что Европейские критерии тесно связаны с "Оранжевой книгой", что делает их не вполне самостоятельным документом.

### Федеральные критерии безопасности информационных технологий

Федеральные критерии безопасности информационных технологий (Federal Criteria for Information Technology Security) разрабатывались как одна из составляющих Американского федерального стандарта по обработке информации (Federal Information Processing Standart), призванного заменить "Оранжевую книгу". Разрботчиками стандарта выступили Национальный институт стандартов и технологий США (National Institute of Standarts and Technology - NIST) и Агенство национальной безопасности США (National Security Agency).

Создание Федеральных критериев безопасности информационных технологий преследовало следующие цели:

1. Определение универсального и открытого для дальнейшего развития *базового набора требований безопасности*, предъявляемых к современным информационным технологиям. Требования к безопасности и критерии оценки уровня защищенности должны соответствовать современному уровню развития информационных технологий и учитывать его прогресс в будущем. Стандарт в этой связи предлагает обоснованный и структурированный подход к разработке требований к продуктам информационных технологий с учетом областей их применения.

2. Совершенствование существующих требований и критериев безопасности. В связи с развитием информационных технологий назрела необходимость пересмотра фундаментальных принципов безопасности с учетом появления новых областей их применения как в государственном, так и в частном секторе.

3. Приведение в соответствие принятых в разных странах требований и критериев безопасности информационных технологий.

4. Нормативное закрепление основополагающих принципов информационной безопасности. Стандарт является обобщением основных принципов обеспечения безопасности информационных технологий, разработанных в 80-е годы, и обеспечивает преемственность по отношению к ним с целью сохранения достижений в области защиты информации.

Федеральные критерии безопасности информационных технологий (далее – Федеральные критерии) охватывают практически полный спектр проблем, связанных с защитой и обеспечением безопасности, т.к. включают все аспекты обеспечения конфиденциальности, целостности и доступности.

Основными объектами применения требований безопасности Федеральных критериев, являются ***продукты информационных технологий*** (Information Technology Products) и ***системы обработки информации*** (Information Technology Systems).

Под **продуктом** информационных технологий (далее – ИТ-продукт) понимается совокупность аппаратных и/или программных средств, которая представляет собой поставляемое конечному потребителю готовое к использованию средство обработки информации. Как правило, ИТ-продукт эксплуатируется не автономно, а интегрируется в систему обработки информации, представляющую собой совокупность ИТ-продуктов, объединенных в функционально полный комплекс, предназначенный для решения прикладных задач. В ряде случаев система обработки информации может состоять только из одного ИТ-продукта, обеспечивающего решение всех стоящих перед системой задач и удовлетворяющего требованиям безопасности.

С точки зрения безопасности принципиальное различие между ИТ‑продуктом и системой обработки информации (СОИ) определяется ***средой их эксплуатации***. Продукт информационных технологий обычно разрабатывается в расчете на то, что он будет использован во многих системах обработки информации, и, следовательно, разработчик должен ориентироваться только на самые общие предположения о среде эксплуатации своего продукта, включающие условия применения и общие угрозы. Напротив, система обработки информации разрабатывается для решения прикладных задач в расчете на требования конечных потребителей, что позволяет в полной мере учитывать специфику воздействий со стороны конкретной среды эксплуатации.

Федеральные критерии содержат положения, относящиеся только к отдельным продуктам информационных технологий. Вопросы построения систем обработки информации из набора ИТ-продуктов не являются предметом рассмотрения этого документа.

Положения Федеральных критериев касаются только собственных средств обеспечения безопасности ИТ-продуктов, т.е. механизмов защиты, встроенных непосредственно в эти продукты в виде соответствующих программных, аппаратных или специальных средств. Для повышения их эффективности могут дополнительно применяться внешние системы защиты и средства обеспечения безопасности, к которым относятся как технические средства, так и организационные меры, правовые и юридические нормы. В конечном счете, безопасность ИТ-продукта определяется совокупностью собственных средств обеспечения безопасности и внешних средств, являющихся частью среды эксплуатации.

Ключевым понятием концепции информационной безопасности Федеральных критериев является понятие ***профиля защиты*** (Protection Profile). **Профиль защиты** – это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его *проектированию, технологии разработки и квалификационному анализу*. Как правило, один *профиль защиты* описывает несколько близких по структуре и назначению ИТ-продуктов. Основное внимание в профиле защиты уделяется требованиям к составу средств защиты и качеству их реализации, а также их адекватности предполагаемым угрозам безопасности.

Федеральные критерии представляют процесс разработки систем обработки информации, начинающийся с формулирования требований потребителями и заканчивающийся введением в эксплуатацию, в виде следующих основных этапов:

1. Разработка и анализ профиля защиты. Требования, изложенные в профиле защиты, определяют функциональные возможности ИТ-продуктов по обеспечению безопасности и условия эксплуатации, при соблюдении которых гарантируется соответствие предъявляемым требованиям. Кроме требований безопасности профиль защиты содержит требования по соблюдению технологической дисциплины в процессе разработки, тестирования и квалификационного анализа ИТ-продукта. Профиль защиты анализируется на полноту, непротиворечивость и техническую корректность.

2. Разработка и квалификационный анализ ИТ-продуктов. Разработанные ИТ-продукты подвергаются *независимому* анализу, целью которого является определение степени соответствия характеристик продукта сформулированным в профиле защиты требованиям и спецификациям.

3. Компоновка и сертификация системы обработки информации в целом. Успешно прошедшие квалификацию уровня безопасности ИТ‑продукты интегрируются в систему обработки информации. Полученная в результате система должна удовлетворять заявленным в профиле защиты требованиям при соблюдении указанных в нем условий эксплуатации.

Федеральные критерии регламентируют только первый этап схемы – разработку и анализ профиля защиты. Процесс создания ИТ-продуктов и компоновка систем обработки информации остаются вне рамок этого стандарта.

### Общие критерии безопасности информационных технологий

Общие критерии безопасности информационных технологий (Common Criteria for Information Technology Security Evaluation, далее – Общие критерии) являются результатом совместных усилий авторов Европейских критериев безопасности информационных технологий, Федеральных критериев безопасности информационных технологий и Канадских критериев безопасности компьютерных систем, направленных на объединение основных положений этих документов и создание единого международного стандарта безопасности информационных технологий.

Версия 2.1 данного стандарта утверждена Международной организацией по стандартизации (ISO) в 1999 году в качестве международного стандарта информационной безопасности **ISO/IEC 15408**.

Первая версия Общих критериев была опубликована 31 января 1996 г. Разработчиками документа выступили Национальный институт стандартов и технологий и Агентство национальной безопасности США, а также соответствующие организации Великобритании, Канады, Финляндии и Нидерландов. Вторая версия вышла в мае 1998 г., причем она отличается от первоначальной довольно существенными исправлениями и дополнениями.

Общие критерии сохраняют совместимость с существующими стандартами и развивают их путем введения новых концепций, соответствующих современному уровню развития информационных технологий, интеграции национальных информационных систем в единое мировое информационное пространство. Общие критерии оперируют уже знакомым понятием ИТ-продукт и используют концепцию профиля защиты.

Общие критерии разрабатывались в расчете на то, чтобы удовлетворить запросы трех групп специалистов, в равной степени являющихся пользователями таких документов: производителей и потребителей продуктов информационных технологий, а также экспертов по оценке уровня их безопасности.

**Производители** должны использовать Общие критерии при проектировании и разработке ИТ-продуктов, а также в подготовке их к квалификационному анализу и сертификации. Этот документ дает возможность производителям на основании анализа запросов потребителя определить набор требований, которым должен удовлетворять разрабатываемый ими продукт. Кроме того, производители могут использовать Общие критерии для определения границ своей ответственности, а также условий, которые необходимо выполнить для успешного прохождения квалификационного анализа и сертификации ими продукта.

**Потребители** используют предлагаемую Общими критериями технологию для обоснования своих претензий на то, что поставляемый им ИТ-продукт успешно противостоит угрозам безопасности, на основании того, что он удовлетворяет выдвинутым функциональным требованиям и их реализация осуществлена с достаточным уровнем адекватности.

**Эксперты** по сертификации используют этот документ в качестве критериев определения соответствия средств защиты ИТ-продукта требованиям, предъявляемым к нему потребителями, и угрозам, действующим в среде его эксплуатации. Общие критерии описывают только общую схему проведения квалификационного анализа и сертификации, но не регламентируют процедуру их осуществления. Вопросам методологии квалификационного анализа и сертификации посвящен отдельный раздел – Общая методология оценки безопасности информационных технологий.

Таким образом, Общие критерии обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

Общие критерии рассматривают информационную безопасность, во‑первых, как совокупность конфиденциальности и целостности, обрабатываемой ИТ-продуктом информации, а также доступности ресурсов ВС, и, во-вторых, ставят перед средствами защиты задачу противодействия угрозам, *актуальным* для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации. Поэтому в концепцию Общих критериев входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.

Общие критерии регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов используя схему, заимствованную из Федеральных критериев. Они предлагают достаточно сложную и бюрократичную концепцию процесса разработки и квалификационного анализа, требующую от потребителей и производителей большой работы по составлению и оформлению весьма объемных и подробных отчетных документов.

Разработчики Общих критериев также продолжили подход Федеральных критериев, направленный на отказ от единой шкалы безопасности и усилили гибкость предложенных в них решений путем введения частично упорядоченных шкал, благодаря чему потребители и производители получили дополнительные возможности по выбору требований и их адаптации к своим прикладным задачам.

Особое внимание стандарт уделяет адекватности реализации функциональных требований, которая обеспечивается как независимым тестированием и анализом ИТ-продукта, так и применением соответствующих технологий на всех этапах его проектирования и разработки.

В целом требования Общих критериев охватывают практически все аспекты безопасности ИТ-продуктов и технологии их создания, а также содержат все исходные материалы, необходимые потребителям и разработчикам для формирования соответствующих документов. Как следствие, требования Общих критериев являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности информационных технологий.

Данный стандарт ознаменовал собой новый уровень стандартизации информационных технологий, подняв его на межгосударственный уровень. За этим проглядывается реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что даст возможности для интеграции национальных информационных систем, а это в свою очередь откроет совершенно новые сферы применения информационных технологий.

## ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий"

ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий" относится к разновидности стандартов, оформленных на основе аутентичного текста. Основой для него стал описанный выше международный стандарт ISO/IEС 15408-99 "Общие критерии безопасности информационных технологий" (далее – Общие критерии или ОК).

Общие критерии состоят из 3-х частей:

1. Введение и общая модель.

2. Функциональные требования безопасности.

3. Требования доверия к безопасности.

Область использования ОК включает как процесс разработки ИТ‑продуктов или АС, так и приобретение коммерческих продуктов и систем. При проведении оценки такой продукт или систему информационных технологий называют *объектом оценки* (ОО), к числу которых ОК относят: ВС, ОС, распределённые системы, вычислительные сети и приложения.

К числу основных пользователей ОК относит следующих физических и юридических лиц:

1. Сотрудников служб безопасности (СБ), ответственных за определение и выполнение политики и требований безопасности организации в области ИТ.

2. Сотрудников, ответственных за техническое состояние оборудования.

3. Аудиторов (внешних и внутренних).

4. Проектировщиков систем безопасности, ответственных за спецификацию систем безопасности и продуктов ИТ.

5. Аттестующих, ответственных за приёмку системы ИТ в эксплуатацию в конкретной среде.

6. Заявителей, заказывающих оценку и обеспечивающих её проведение.

7. Органы оценки, ответственных за руководство и надзор за программами проведения оценок безопасности ИТ.

**Часть 1** стандарта включает методологию оценки безопасности ИТ, определяет виды требований безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах трёх категорий пользователей: потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности ОО по методологии Общих критериев определяются исходя из целей безопасности, которые, в свою очередь, основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

В первой части определено от чего надо защищать информацию:

от несанкционированного раскрытия (конфиденциальность);

от модификации (целостность);

от потери возможности её использования (доступность).

**Часть 2** стандарта включает универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определённым правилам.

**Часть 3** стандарта включает систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. В этой же части содержится описание *оценочных уровней доверия*, определяющих шкалу требований, которые позволяют с возрастающей степенью полноты и строгости провести оценку проектной, тестовой и эксплуатационной документации, правильности функционирования комплекса средств безопасности, оценку уязвимостей продукта или системы ИТ, стойкости механизмов защиты и сделать заключение об уровне безопасности объекта оценки.

Некоторые вопросы рассматриваются как лежащие вне области действия ОК, поскольку они требуют привлечения специальных методов или являются смежными по отношению к безопасности ИТ. Часть из них перечислена ниже.

Стандарт не содержит критериев оценки безопасности, касающихся *административных мер безопасности* (организационные меры, управление персоналом, физическая защита и процедурный контроль), непосредственно не относящихся к мерам безопасности ИТ.

Оценка специальных физических аспектов безопасности ИТ, таких как контроль электромагнитного излучения, прямо не затрагивается, хотя многие концепции ОК применимы и в этой области. В частности, рассмотрены некоторые аспекты физической защиты ОО.

В ОК не рассматривается ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки и сертификации. Тем не менее, ожидается, что ОК будут использоваться для целей оценки в контексте такой структуры и такой методологии.

Процедуры использования результатов оценки при аттестации продуктов и систем ИТ находятся вне области действия ОК. Аттестация продукта или системы ИТ является административным процессом, посредством которого предоставляются полномочия на их использование в конкретной среде эксплуатации.

Критерии для оценки специфических качеств криптографических алгоритмов также не входят в ОК. Если требуется независимая оценка математических свойств криптосистем, встроенной в ОО, то в системе оценки, в рамках которой применяются ОК, необходимо предусмотреть проведение таких оценок.

ОК определяют следующий перечень сокращений, являющихся обязательными для всех частей стандарта.

ЗБ (ST) – задание по безопасности;

ИТ (IT) – информационная технология;

ИФБО (TSFI) – интерфейс ФБО;

ОДФ (TSC) – область действия ФБО;

ОК (CC) – общие критерии;

ОО (TOE) – объект оценки;

ОУД (EAL) – оценочный уровень доверия;

ПБО (TSP) – политика безопасности ОО;

ПЗ (РР) – профиль защиты;

ПФБ (SFP) – политика функции безопасности;

СФБ (SOF) – стойкость функции безопасности;

ФБ (SF) – функция безопасности;

ФБО (TSF) – функция безопасности ОО.

### 

### Часть 1. Введение и общая модель

Первая часть стандарта включает описание рассмотренной выше структуры стандарта в целом, области его применения, список основных сокращений. Далее описывается используемый глоссарий, он представлен в табл.

Таблица

Глоссарий Общих критериев

| № | Термин | Смысловое содержание | Английский эквивалент |
| --- | --- | --- | --- |
| 1. | **Активы** | Информация или ресурсы, подлежащие защите контрмерами ОО | **Assets** |
| 2. | **Атрибут безопасности** | Информация, связанная с субъектами, пользователями и/или объектами, которая используется для осуществления ПБО | **Security attribute** |
| 3. | **Аутентификаци-онные данные** | Информация, используемая для верификации предъявленного идентификатора пользователя | **Authentication data** |
| 4. | **Базовая СФБ** | Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения | **SOF-basic** |
| 5. | **Внешний объект ИТ** | Любые продукт или система ИТ, доверенные или нет, находящиеся вне ОО и взаимодействующие с ним | **External IT entity** |
| 6. | **Выбор** | Выделение одного или нескольких элементов из перечня в компоненте | **Selection** |
| 7. | **Внутренний канал связи** | Канал связи между разделёнными частями ОО | **Internal communication channel** |
| 8. | **Высокая СФБ** | Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения | **SOF-high** |
| 9. | **Данные ФБО** | Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО | **TSF data** |
| 10. | **Данные пользователя** | Данные, созданные пользователем и для пользователя, которые не влияют на выполнение ФБО | **User data** |
| 11. | **Доверенный канал** | Средство взаимодействия между ФБО и удалённым доверенным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании ПБО | **Trusted channel** |
| 12. | **Доверенный маршрут** | Средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую степень уверенности в поддержании ПБО | **Trusted path** |
| 13. | **Доверие** | Основание для уверенности в том, что сущность отвечает своим целям безопасности | **Assurance** |
| 14. | **Зависимость** | Соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть, как правило, удовлетворено, чтобы и другие требования могли бы отвечать своим целям | **Dependency** |
| 15. | **Задание по безопасности** | Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО | **Security target** |
| 16. | **Идентификатор** | Представление уполномоченного пользователя (например, строка символов), однозначно его идентифицирующее. Таким представлением может быть либо полное или сокращённое имя этого пользователя, либо его псевдоним | **Identity** |
| 17. | **Интерфейс функций безопасности ОО** | Совокупность интерфейсов, как интерактивных (человеко-машинные интерфейсы), так и программных (интерфейсы прикладных программ), с использованием которых осуществляется доступ к ресурсам ОО при посредничестве ФБО или получение от ФБО какой-либо информации | **TOE security functions interface** |
| 18. | **Итерация** | Более чем однократное использование компонента при различном выполнении операций | **Iteration** |
| 19. | **Класс** | Группа семейств, объединённых общим назначением | **Class** |
| 20. | **Компонент** | Наименьшая выбираемая совокупность элементов, которая может быть включена в ПЗ, ЗБ или пакет | **Component** |
| 21. | **Механизм проверки правомочности обращений** | Реализация концепции монитора обращений, обладающая следующими свойствами: защищённостью от проникновения; постоянной готовностью; простотой, достаточной для проведения исчерпывающего анализа и тестирования | **Reference validation mechanism** |
| 22. | **Модель политики безопасности ОО** | Структурированное представление политики безопасности, которая должна быть осуществлена ОО | **TOE security policy model** |
| 23. | **Монитор обращений** | Концепция абстрактной машины, осуществляющей политику управления доступом ОО | **Reference monitor** |
| 24. | **Назначение** | Спецификация определённого параметра в компоненте | **Assignment** |
| 25. | **Неформальный** | Выраженный на естественном языке | **Informal** |
| 26. | **Область действия ФБО** | Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО | **TSF scope of control** |
| 27. | **Объект** | Сущность в пределах ОДФ, которая содержит или получает информацию и над которой субъекты выполняют операции | **Object** |
| 28. | **Объект оценки** | Подлежащие оценке продукт ИТ или система с руководствами администратора и пользователя | **Target of evaluation** |
| 29. | **Орган оценки** | Организация, которая посредством системы оценки обеспечивает реализацию ОК для определённого сообщества и в связи с этим устанавливает стандарты и контролирует качество оценок, проводимых организациями в пределах данного сообщества | **Evaluation authority** |
| 30. | **Оценка** | Оценка ПЗ, ЗБ или ОО по определённым критериям | **Evaluation** |
| 31. | **Оценочный уровень доверия** | Пакет компонентов доверия из части 3 настоящего стандарта, представляющий некоторое положение на предопределённой в стандарте шкале доверия | **Evaluation assurance level** |
| 32. | **Пакет** | Предназначенная для многократного использования совокупность функциональных компонентов или компонентов доверия (например, ОУД), объединённых для удовлетворения совокупности определённых целей безопасности | **Package** |
| 33. | **Передача в пределах ОО** | Передача данных между разделёнными частями ОО | **Internal TOE transfer** |
| 34. | **Передача за пределы области действия ФБО** | Передача данных сущностям, не контролируемым ФБО | **Transfer outside TSF control** |
| 35. | **Передача между ФБО** | Передача данных между ФБО и функциями безопасности других доверенных продуктов ИТ | **Inter-TSF transfers** |
| 36. | **Политика безопасности организации** | Одно или несколько правил, процедур, практических приёмов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности | **Organizational security policies** |
| 37. | **Политика безопасности ОО** | Совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОО | **TOE security policy** |
| 38. | **Политика функции безопасности** | Политика безопасности, осуществляемая ФБ | **Security function policy** |
| 39. | **Полуфор-мальный** | Выраженный на языке с ограниченным синтаксисом и определённой семантикой | **Semiformal** |
| 40. | **Пользователь** | Любая сущность (человек-пользователь или внешний объект ИТ) вне ОО, которая взаимодействует с ОО | **User** |
| 41. | **Потенциал нападения** | Прогнозируемый потенциал для успешного (в случае реализации) нападения, выраженный в показателях компетентности, ресурсов и мотивации нарушителя | **Attack potential** |
| 42. | **Продукт** | Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определённые функциональные возможности и предназначенная для непосредственного использования или включения в различные системы | **Product** |
| 43. | **Профиль защиты** | Независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя | **Protection profile** |
| 44. | **Расширение** | Добавление в ЗБ или ПЗ функциональных требований, не содержащихся в части 2 настоящего стандарта, и/или требований доверия, не содержащихся в части 3 настоящего стандарта | **Extension** |
| 45. | **Ресурс ОО** | Всё, что может использоваться или потребляться в ОО | **TOE resource** |
| 46. | **Роль** | Заранее определённая совокупность правил, устанавливающих допустимое взаимодействие между пользователем и ОО | **Role** |
| 47. | **Связность** | Свойство ОО, позволяющее ему взаимодействовать с объектами ИТ, внешними по отношению к ОО. Это взаимодействие включает обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации | **Connectivity** |
| 48. | **Секрет** | Информация, которая должна быть известна только уполномоченным пользователям и/или ФБО для осуществления определённой ПФБ | **Secret** |
| 49. | **Семейство** | Группа компонентов, которые объединены одинаковыми целями безопасности, но могут отличаться акцентами или строгостью | **Family** |
| 50. | **Система** | Специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации | **System** |
| 51. | **Система оценки** | Административно-правовая структура, в рамках которой в определённом обществе органы оценки применяют ОК | **Evaluation scheme** |
| 52. | **Средняя СФБ** | Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения | **SOF-medium** |
| 53. | **Стойкость функции безопасности** | Характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения её ожидаемого безопасного поведения при прямой атаке на лежащие в её основе механизмы безопасности | **Strength of function** |
| 54. | **Субъект** | Сущность в пределах ОДФ, которая инициирует выполнение операций | **Subject** |
| 55. | **Уполномочен-ный пользователь** | Пользователь, которому в соответствии с ПБО разрешено выполнять какую-либо операцию | **Authorized user** |
| 56. | **Усиление** | Добавление одного или нескольких компонентов доверия из части 3 настоящего стандарта в ОУД или пакет требований доверия | **Augmentation** |
| 57. | **Уточнение** | Добавление деталей в компонент | **Refinement** |
| 58. | **Функции безопасности ОО** | Совокупность всех функций безопасности ОО, направленных на осуществление ПБО | **TOE security functions** |
| 59. | **Функция безопасности** | Функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО | **Security function** |
| 60. | **Формальный** | Выраженный на языке с ограниченным синтаксисом и определённой семантикой, основанной на установившихся математических понятиях | **Formal** |
| 61. | **Человек-пользователь** | Любое лицо, взаимодействующее с ОО | **Human user** |
| 62. | **Цель безопасности** | Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям | **Security objective** |
| 63. | **Элемент** | Неделимое требование безопасности | **Element** |

Хотя ОК не предписывают конкретную методологию разработки или модель жизненного цикла, они, тем не менее представляют некоторые основополагающие предположения о соотношениях между требованиями безопасности и собственно разрабатываемым ОО. В основе данной методологии лежит *уточнение требований безопасности*, сведенных в краткую спецификацию в составе задания по безопасности, являющегося по сути исходным документом для разработки и последующей оценки (фактически некий аналог ТЗ). Каждый последующий уровень уточнения представляет декомпозицию проекта с его дополнительной детализацией. Наиболее подробным (и наименее абстрактным) представлением в итоге является непосредственно реализация ОО.

Количество уровней детализации при этом зависит от уровня доверия, который требуется обеспечить. В ОК предусмотрены следующие промежуточные этапы детализации, формируемые на основе задания по безопасности: функциональная спецификация, проект верхнего уровня, проект нижнего уровня и реализация.

С методологией создания ОО тесно связан процесс его оценки, который может проводиться как параллельно с разработкой, так и после ее окончания. Основными исходными материалами для оценки ОО являются:

совокупность материалов, характеризующих ОО, включая прошедшее оценку ЗБ в качестве основы;

сам ОО, безопасность которого требуется оценить;

критерии, методология и система оценки.

Кроме того, в качестве исходных материалов для оценки возможно также использование вспомогательных материалов и специальных знаний в области безопасности ИТ, которыми располагает оценщик и сообщество участников оценок.

Ожидаемым результатом оценки является *подтверждение удовлетворения объектом оценки требований безопасности*, изложенных в его ЗБ, а также один или несколько отчетов, документирующих выводы оценщика относительно ОО, сделанные в соответствии с критериями оценки. Такие отчеты, помимо разработчика, очевидно, будут полезны также реальным и потенциальным потребителям продукта или системы.

Таким образом, *основой* разработки и эксплуатации любого ОО в Общих критериях провозглашается *совокупность требований безопасности*.

В ОК определены 3 группы конструкций для описания требований безопасности: пакет, профиль защиты (ПЗ) и задание по безопасности (ЗБ).

*Пакет* представляет собой некую промежуточную комбинацию компонентов безопасности. Он предназначен для многократного использования и определяет требования, которые известны как полезные и эффективные для достижения некоторых установленных целей. Допускается применение пакета при создании более крупных пакетов, профилей защиты и заданий по безопасности.

*Профиль защиты* содержит совокупность требований безопасности, взятых из ОК или сформулированных в явном виде. ПЗ позволяет выразить независимые от конкретной реализации требования безопасности для *некоторой совокупности ОО*, которые полностью согласуются с набором целей безопасности. ПЗ также предназначен для многократного использования и определения как функциональных требований, так и требований доверия к ОО, которые полезны и эффективны для достижения установленных целей. ПЗ также содержит логическое обоснование требований и целей безопасности.

*Задание по безопасности* содержит совокупность требований безопасности, которые могут быть определены ссылками на ПЗ, непосредственно на функциональные компоненты или компоненты доверия или же сформулированы в явном виде. ЗБ позволяет выразить требования безопасности для *конкретного ОО*, которые по результатам оценки ЗБ признаны полезными и эффективными для достижения установленных целей безопасности. ЗБ является основой для соглашения между всеми сторонами относительно того, какую безопасность предлагает ОО.

В первой части ОК подробно описан и процесс формирования требований безопасности, поскольку данные требования, выраженные в итоге в ЗБ, должны быть обоснованы и непротиворечивы, достаточны, после чего только на их основе производится оценка ОО.

В соответствии с ОК на основании исследования политик безопасности, угроз и рисков должны быть сформированы следующие материалы, относящиеся к безопасности:

изложение предположений, которым удовлетворяла бы среда разрабатываемой ИТ для того, чтобы она считалась безопасной;

изложение угроз безопасности активов, в котором были бы идентифицированы все угрозы, при этом угрозы раскрываются через понятия агента угрозы (нарушителя), предполагаемого метода нападения, любых уязвимостей, которые являются предпосылкой для нападения, и идентификации активов, которые являются целью нападения;

изложение политики безопасности, применяемой в организации, для системы ИТ такая политика может быть описана достаточно точно, тогда как для продуктов ИТ общего предназначения или класса продуктов о политике безопасности организации могут быть сделаны, при необходимости, только рабочие предположения.

Результаты анализа среды безопасности затем должны использоваться для установления *целей безопасности*, которые направлены на противостояние установленным угрозам, а также проистекают из установленной политики безопасности организации и сделанных предположений. Необходимо, чтобы цели безопасности были согласованы с определенными ранее целями применения или предназначением продукта, а также со сведениями о физической среде.

*Требования безопасности* являются результатом преобразования целей безопасности в совокупность требований безопасности для объекта оценки и требований безопасности для среды, которые, в случае их удовлетворения, обеспечат для него способность достижения его целей безопасности.

Имеется две различные категории требований безопасности – функциональные требования и требования доверия.

*Функциональные требования* налагаются на те функции, которые предназначены для поддержания безопасности ОО и определяют желательный безопасный режим функционирования. Примерами функциональных требований являются требования к идентификации, аутентификации, аудиту безопасности и т.д.

*Требования доверия* налагаются на действия разработчика, представленные свидетельства и действия оценщика. Примерами требований доверия являются требования к строгости процесса разработки, по поиску потенциальных уязвимостей и анализу их влияния на безопасность.

Требования безопасности обычно включают как требования наличия желательных режимов функционирования, так и требования отсутствия нежелательных режимов. Наличие желательного режима обычно можно продемонстрировать путем непосредственного применения или испытаний (тестирования). Не всегда удается убедительно продемонстрировать отсутствие нежелательного режима. Уменьшению риска наличия нежелательного режима в значительной мере способствуют испытания (тестирование), экспертиза проекта и окончательной реализации.

### Часть 2. Функциональные требования безопасности

Вторая часть стандартаопределяет функциональные требования безопасности ИТ объекта оценки, которые предназначены для достижения целей безопасности, установленных в ПБ и ЗБ. В этой части перечисляются функциональные требования безопасности, которые могут быть предъявлены к объекту оценки. Оценка ОО касается прежде всего, подтверждения того, что в отношении ресурсов ОО осуществляется определённая политика безопасности. Стандарт подчёркивает, что политика безопасности ОО (ПБО) состоит из различных политик функций безопасности (ПФБ).

В соответствии с ОК организация требований безопасности осуществляется в виде иерархии: *класс – семейство – компонент – элемент*.

Термин *класс* применяется для общего группирования требований безопасности. Составляющие класса называются *семействами*, под которыми понимается группа наборов требований безопасности, имеющих общие цели безопасности, но различающихся акцентами или строгостью. Составляющие семейства называются *компонентами*, которые представляют специфический набор требований безопасности, который является наименьшим выбираемым набором требований безопасности для включения в структуры, определяемые ОК. Компоненты составлены из отдельных *элементов*. Каждый элемент определяет требования безопасности на самом нижнем уровне. Он является тем неделимым требованием безопасности, которое может быть верифицировано при оценке.

Для идентификации функционального элемента вводится краткая уникальная запись. Например, запись имени функционального элемента FDP\_IFF.4.2 читается следующим образом:

F – функциональное требование;

DP – класс "Защита данных пользователя";

IFF – семейство "Функции управления информационными потоками";

4 – 4-ый компонент "Частичное устранение неразрешённых информационных потоков";

2 – 2-ой элемент компонента.

ОК предусматривают 11 классов функциональных требований:

FAU – аудит безопасности;

FCO – связь;

FCS – криптографическая поддержка;

FDP – защита данных пользователя;

FIA – идентификация и аутентификация;

FMT – управление безопасностью;

FPR – приватность;

FPT – защита ФБО;

FRU – использование ресурсов;

FTA – доступ к ОО;

FTP – доверенный маршрут/канал.

Класс **FAU** (аудит безопасности) включает распознавание, запись, хранение и анализ информации, связанной с действиями, например с действиями, контролируемыми в соответствии с политикой безопасности объекта оценки. Этот класс включает 6 семейств:

автоматическая реакция аудита безопасности (FAU\_ARP);генерация данных аудита безопасности (FAU\_GEN);анализ аудита безопасности (FAU\_SAA);просмотр аудита безопасности (FAU\_SAR);выбор событий аудита безопасности (FAU\_SEL);хранение данных аудита безопасности (FAU\_STG).

Класс **FCO** (связь) содержит два семейства, связанные с обеспечением идентификаторов сторон, участвующих в обмене данными:

идентификатор отправителя переданной информации (FCO\_NRO – доказательство отправления);

идентификатор получателя переданной информации (FCO\_NRR – доказательство получения).

Класс **FCS** (криптографическая поддержка) используется, когда объект оценки имеет криптографические функции, реализованные аппаратными, программно-аппаратными и/или программными средствами. Реализация целей этого класса должна обеспечивать: идентификацию, аутентификацию, неотказуемость сообщения, доверенный маршрут, доверенный канал, разделение данных.

Класс состоит из двух семейств:

управление криптографическими ключами (FCS\_CKM);

криптографические операции (FCS\_COP).

Класс **FDP** (защита данных пользователя) определяет требования к функциям безопасности объекта, связанным с защитой данных пользователя. Класс имеет 13 семейств, разбитых на 4 группы.

1. Политика функций безопасности ОО для защиты данных пользователя, включает 2 семейства:

политика управления доступом (FDP\_ACC);политика управления информационными потоками (FDP\_IFC).

2. Виды защиты данных пользователя, включает 6 семейств:

функции управления доступом (FDP\_ACF);функции управления информационными потоками (FDP\_IFF);передача в пределах ОО (FDP\_ITT);защита остаточной информации (FDP\_RIP);откат (FDP\_ROL);целостность хранимых данных (FDP\_SDI).

3. Автономное хранение, импорт и экспорт данных, включает 3 семейства:

аутентификация данных (FDP\_DAU);экспорт данных за пределы действий ФБО (FDP\_ETC);импорт данных из-за пределов действия ФБО (FDP\_ITC).

4. Связь между ФБО, имеет 2 семейства:

защита конфиденциальности данных пользователя при передаче между ФБО (FDP\_UCT);

защита целостности данных пользователя при передаче между ФБО (FDP\_UIT).

Класс **FIA** (идентификация и аутентификация) обеспечивает связь пользователей с соответствующими атрибутами безопасности (идентификатор группы, уровень безопасности или целостности). Класс включает 6 семейств:

отказы аутентификации (FIA\_AFL);определение атрибутов пользователя (FIA\_ATD);спецификация секретов (FIA\_SOS);аутентификация пользователя (FIA\_UAU);

идентификация пользователя (FIA\_UID);связывание пользователь-субъект (FIA\_USB).

Класс **FMT** (управление безопасностью) предназначен для спецификации управления некоторыми аспектами ФБО: атрибутами безопасности, данными и отдельными функциями. Класс включает 6 семейств:

управление отдельными функциями ФБО (FMT\_MOF);управление атрибутами безопасности (FMT\_MSA);управление данными ФБО (FMT\_MTD);отмена (FMT\_REY);

срок действия атрибута безопасности (FMT\_SAE);роли управления безопасностью (FMT\_SMR).

Класс **FPR** (приватность) предоставляет пользователю защиту от раскрытия его идентификатора и злоупотребления этим другими пользователями. Класс содержит 4 семейства:

анонимность (FPR\_ANO);псевдонимность (FPR\_PSE);невозможность ассоциации (FPR\_UNL);скрытность (FPR\_UNO).

Класс **FPT** (защита ФБО) содержит функциональные требования, которые связаны с целостностью и управлением механизмами, реализованными в ФБО. По сути, требования этого класса дублируют требования из класса FDP (защита данных пользователя), однако, они специализированы на защиту данных пользователя, а класс FPT нацелен на защиту данных функций безопасности объекта. Класс FPT содержит 16 семейств:

тестирование базовой абстрактной машины (FPT\_AMT); безопасность при сбое (FPT\_FLS); доступность экспортируемых данных ФБО (FPT\_ITA); конфиденциальность экспортируемых данных ФБО (FPT\_ITO); целостность экспортируемых данных ФБО (FPT\_ITI); передача данных ФБО в пределах ОО (FPT\_ITT); физическая защита ФБО (FPT\_PHP); надёжное восстановление (FPT\_RCV); обнаружение повторного использования (FPT\_RPL); посредничество при обращениях (FPT\_RVM); разделение домена (FPT\_SEP); протокол синхронизации состояний (FPT\_SSP);метки времени (FPT\_STM);согласованность данных ФБО между ФБО (FPT\_TDC);согласованность данных ФБО при дублировании в пределах ОО (FPT\_TDC);самотестирование (FPT\_TST).

Класс **FRU** (использование ресурсов) поддерживает доступность требуемых ресурсов (вычислительные возможности, память) и состоит из 3 семейств:

отказоустойчивость (FRU\_FLT); приоритет обслуживания (FRU\_PRS); распределение ресурсов (FRU\_RSA).

Класс **FTA** (доступ к ОО) определяет требования к управлению открытием сеанса пользователя и состоит из 6 семейств:

ограничение области выбираемых атрибутов (FTA\_LSA); ограничение на параллельные сеансы (FTA\_MCS); блокирование сеанса (FTA\_SSL); предупреждения перед предоставлением доступа к ОО (FTA\_TAB); история доступа к ОО (FTA\_TAB); открытие сеанса с ОО (FTA\_TSE).

Класс **FTP** (доверенный маршрут/канал) определяет требования как к доверенному маршруту связи между пользователями и ФБО, так и к доверенному каналу связи ФБО и другими доверенными продуктами ИТ.

Под доверенным каналом понимается канал связи, который может быть инициирован любой из связывающихся сторон и обеспечивает неотказываемые характеристики, связанные с идентификаторами сторон канала. Класс содержит два семейства:

доверенный канал передачи между ФБО (FTP\_ITC);

доверенный маршрут (FTP\_TRP).

### Часть 3. Требования доверия к безопасности

Третья частьстандарта содержит систематизированный каталог функциональных требований доверия, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Стандарт определяет, что *способом достижения доверия является оценка*.

В качестве основных методов для проведения оценки используют:

анализ и проверку процессов и процедур;

проверку, что процессы и процедуры действительно применяются;

анализ соответствия между представлениями проекта ОО;

анализ соответствия каждого представления проекта ОО требованиям;

верификацию доказательств;

анализ руководств;

анализ разработанных функциональных тестов и полученных результатов;

независимое функциональное тестирование;

анализ уязвимостей, включающий предположения о недостатках;

тестирование проникновения.

Требования доверия строятся аналогично функциональным требованиям в виде иерархии:класс – семейство – компонент – элемент. Каждому классу присваивается уникальное имя, которое указывает на тематические разделы, на которые распространяется данный класс доверия. Имя начинается с буквы "А", за которой следуют ещё две буквы латинского алфавита, относящиеся к имени класса.

Помимо классов, определяющих требования доверия, ОК также описывают три класса требований по поддержке доверия, оценке профиля защиты и задания по безопасности.

Класс **AMA** (поддержка доверия) содержит 4 семейства:

план поддержки доверия (AMA\_AMP);отчёт о категорировании компонентов ОО (AMA\_CAT);свидетельство о поддержке доверия (AMA\_EVD);анализ влияния на безопасность (AMA\_SIA).

Класс **APE** (оценка профиля защиты) включает 6 семейств:

профиль защиты, введение ПЗ (APE\_INT);профиль защиты, описание ОО (APE\_DES);профиль защиты, среда безопасности (APE\_ENV);профиль защиты, цели безопасности (APE\_OBJ);профиль защиты, требования безопасности ИТ (APE\_REQ);профиль защиты, требования безопасности ИТ, сформулированные в явном виде (APE\_SRE).

Класс **ASE** (оценка задания по безопасности) включает 8 семейств:

задание по безопасности, введение ЗБ (ASE\_INT);задание по безопасности, описание ОО (ASE\_DES);задание по безопасности, среда безопасности (ASE\_ENV);задание по безопасности, цели безопасности (ASE\_OBJ);задание по безопасности, требования безопасности ИТ (ASE\_REQ);задание по безопасности, утверждение о соответствии ПЗ (ASE\_PPC);задание по безопасности, краткая спецификация ОО (ASE\_TSS);задание по безопасности, требования безопасности ИТ, сформулированные в явном виде (ASE\_SRE).

Требования для оценки профиля защиты и задания по безопасности также трактуются как классы доверия, структура которых подобна структуре других классов доверия. Отличие заключается лишь в отсутствии подраздела ранжирования компонентов в описаниях семейств. Причина в том, что каждое семейство имеет только один компонент и, следовательно, ранжирование отсутствует.

Особое внимание в 3-й части ОК уделено используемым *оценочным уровням доверия* (ОУД). ОУД образуют возрастающую шкалу, которая позволяет соотнести получаемый уровень доверия со стоимостью и возможностью достижения этой степени доверия.

В стандарте определены *семь* упорядоченных оценочных уровней доверия для ранжирования доверия к ОО. Они иерархически упорядочены, поскольку каждый ОУД представляет более высокое доверие, чем любой из предыдущих ОУД. Увеличение доверия от ОУД1 к ОУД7 достигается заменой какого-либо компонента доверия иерархически более высоким компонентом из того же семейства доверия (т.е. увеличением строгости, области и/или глубины оценки) и добавлением компонентов доверия из других семейств доверия (т.е. добавлением новых требований).

ОУД состоят из определённой комбинации компонентов доверия. Точнее, каждый ОУД включает не больше, чем один компонент каждого семейства доверия, а все зависимости каждого компонента доверия учтены.

Важно обратить внимание, что не все семейства и компоненты доверия и поддержки доверия включены в оценочные уровни доверия. Это не означает, что они не обеспечивают значимое и полезное доверие. Напротив, ожидается, что эти семейства и их компоненты будут рассматриваться для усиления ОУД в тех ПЗ и ЗБ, для которых они полезны.

Хотя в стандарте определены именно ОУД, можно представлять другие комбинации компонентов доверия. Для этого специально введено понятие "усиление" (augmentation), которое предполагает добавление компонентов доверия из семейств доверия, до этого не включённых в некоторый ОУД, или замену компонентов доверия в некотором ОУД другими, иерархически более высокими компонентами доверия из этого же самого семейства доверия. Вводящий усиление обязан строго обосновать полезность и дополнительную ценность добавленного к ОУД компонента доверия. ОУД может быть также расширен требованиями доверия, сформулированными в явном виде.

Таким образом, ОУД могут быть усилены и не могут быть ослаблены. Например, понятие "ОУД за исключением какого-либо составляющего его компонента доверия" не признаётся в стандарте как допустимое утверждение.

Методология и требования ОК не охватывают вопросов организации процессов оценки (сертификации и/или аттестации). Это является предметом ведения государственных органов. В нашей стране в сфере защиты информации деятельность такой системы регулируется ФСТЭК на основе выпускаемых ею руководящих документов.

## 

Гостехкомиссия России вела весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии".

Рассмотрим два важных Руководящих документа – Классификацию **автоматизированных систем (АС)** по уровню **защищенности от несанкционированного доступа (НСД)** и аналогичную Классификацию **межсетевых экранов (МЭ)**.

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса – 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

**Классификации межсетевых экранов** — представляется принципиально важным, поскольку в нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Данный РД важен не столько содержанием, сколько самим фактом своего существования. РД получил высокую оценку не только в России, но и в мире.

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется **фильтрация информации**. Чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

**Рекомендации Х.800**

Технические спецификации X.800, появились немногим позднее "Оранжевой книги", но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации X.800 – документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

**Аутентификация.** Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

**Управление доступом.** Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

**Конфиденциальность данных.** Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем **конфиденциальность трафика** (это защита информации, которую можно получить, анализируя сетевые потоки данных).

**Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

**Неотказуемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является **аутентификация источника данных**.

В следующей таблице указаны уровни **эталонной семиуровневой модели** OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

### Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

* **шифрование**;
* **электронная цифровая подпись**;
* механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
* механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
* механизмы аутентификации. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
* механизмы **дополнения трафика**;
* механизмы **управления маршрутизацией**. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
* механизмы **нотаризации**. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

### Администрирование средств безопасности

**Администрирование средств безопасности** включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение **криптографических ключей**, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для реализации избранной политики безопасности.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

* администрирование информационной системы в целом;
* администрирование сервисов безопасности;
* администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, **реагирование** на происходящие события, **аудит** и **безопасное восстановление**.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

* **управление ключами (генерация и распределение)**;
* **управление шифрованием** (установка и синхронизация криптографических параметров). К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению;
* администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т.п.);
* управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т.п.);
* управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т.п.);
* управление маршрутизацией (выделение доверенных путей);
* управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

### Стандарты ISO/IEC 17799:2002 (BS 7799:2000) – ГОСТ Р ИСО/МЭК 17799

Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «**Управление информационной безопасностью — Информационные технологии**» (Information technology — Information security management») является одним из наиболее известных стандартов в области защиты информации. Данный стандарт был разработан на основе первой части Британского стандарта BS 7799-1:1995 «Практические рекомендации по управлению информационной безопасностью» (Information security management — Part 1: Code of practice for information security management») и относится к новому поколению стандартов информационной безопасности компьютерных ИС.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

* необходимость обеспечения информационной безопасности;
* основные понятия и определения информационной безопасности;
* политика информационной безопасности компании;
* организация информационной безопасности на предприятии;
* классификация и управление корпоративными информационными ресурсами;
* кадровый менеджмент и информационная безопасность;
* физическая безопасность;
* администрирование безопасности КИС;
* управление доступом;
* требования по безопасности к КИС в ходе их разработки, эксплуатации и сопровождения;
* управление бизнес-процессами компании с точки зрения информационной безопасности;
* внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799—2:2000 «Спецификации систем управления информационной безопасностью» («Information security management — Part 2: Specification for information security management systems»), определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита ИС.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов — British Standards Institution (BSI), изданные в 1995—2003 гг. в виде следующей серии:

* «Введение в проблему управления информационной безопасностью» (Information security managment: an introduction»);
* «Возможности сертификации на требования стандарта BS 7799» («Preparing for BS 7799 sertification»);
* «Руководство BS 7799 по оценке и управлению рисками» («Guide to BS 7799 risk assessment and risk management);
* «Руководство для проведения аудита на требования стандарта» («BS 7799 Guide to BS 7799 auditing»);
* «Практические рекомендации по управлению безопасностью информационных технологий» («Code of practice for IT management).

В 2002 г. международный стандарт ISO 17799 (BS 7799) был пересмотрен и существенно дополнен. В новом варианте этого стандарта большое внимание уделено вопросам повышения культуры защиты информации в различных международных компаниях.

**Международный стандарт ISO 27001 -** **ГОСТ Р ИСО/МЭК 27001** "Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (этот стандарт принят 31 декабря 2006 г.);

Начиная с осени 2005 г. в России все большую известность при построении корпоративных систем менеджмента информационной безопасностью (СМИБ) завоевывает международный стандарт ISO/IEC 27001:2005 "Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

Принят в России в 2006 году как ГОСТ Р ИСО/МЭК 27001.

Истоки ISO/IEC 27001:2005 находятся в британском государственном стандарте BS 7799, который был разработан в 1995 г. Британским институтом стандартов и ведущими организациями и компаниями Великобритании. В 1999-м первая часть BS 7799 была передана в Международную организацию по стандартизации (ISO - The International Organization for Standardization) и в 2000-м утверждена в качестве международного стандарта как ISO/IEC 17799:2000 (BS 7799-1:2000). Следующей его версией стал стандарт ISO/IEC 17799:2005. В 1999 г. вышла в свет вторая часть британского стандарта: BS 7799-2:1999 Information Security management - Specification for ISMS (ISMS - Information Security Management System). В 2002 г. появилась новая, усовершенствованная редакция стандарта - BS 7799-2:2002. На ее основе 14 октября 2005-го был принят стандарт ISO/IEC 27001:2005 . Ожидается развитие серии стандартов 27000 и выпуск ISO/IEC 27002, который сменит ISO/IEC 17799:2005.

Выполнение требований ISO/IEC 27001:2005 позволяет организациям формализовать и структурировать процессы управления ИБ по следующим направлениям:

- разработка политики ИБ;

- организация ИБ;

- организация управления внутренними активами и ресурсами компании, составляющими основу ее ключевых бизнес-процессов;

- защита персонала и снижение внутренних угроз компании;

- физическая безопасность в компании и безопасность окружающей среды;

- управление средствами связи и эксплуатацией оборудования;

- разработка и обслуживание аппаратно-программных систем;

- управление непрерывностью бизнес-процессов в компании;

- соблюдение правовых норм по безопасности.

Цели и комплексы мероприятий ISO/IEC 27001:2005 по каждому направлению работ были заимствованы из стандарта ISO/IEC 17799:2005 (разделы 5-15) и перечислены в его приложении А (Annex A. Control objectives and controls).

**Семейство Международных Стандартов на Системы Управления Информационной Безопасностью 27000** разрабатывается ISO/IEC JTC 1/SC 27. Это семейство включает в себя Международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

Для этого семейства стандартов используется последовательная схема нумерации, начиная с 27000 и далее.

|  |  |
| --- | --- |
| **ISO27000** | Определения и основные принципы. Планируется унификация со стандартами  COBIT и ITIL. Проект стандарта находится в разработке. |
| **ISO27001** | ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). Выпущен в июле 2005 г. |
| **ISO27002** | ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью (ранее ISO/IEC 17799:2005). |
| **ISO27003** | Руководство по внедрению системы управления информационной безопасностью. Выпуск запланирован на 2007 г. |
| **ISO27004** | Измерение эффективности системы управления информационной безопасностью. Выпуск запланирован на 2007 г. |
| **ISO27005** | Управление рисками информационной безопасности (на основе BS 7799-3:2006). Выпуск запланирован на 2007 г. |
| **ISO27006** | ISO/IEC 27006:2007 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью |
| **ISO27007** | Руководство для аудитора СУИБ (в разработке). |
| **ISO27011** | Руководство по управлению информационной безопасностью для телекоммуникаций (в разработке). |

**ISO** (Международная Организация по Стандартизации) и **IEC** (Международная Электротехническая Комиссия) формируют специализированную систему всемирной стандартизации. Государственные органы, являющиеся членами ISO или IEC, участвуют в разработке Международных Стандартов через технические комитеты, созданные соответствующей организацией для стандартизации отдельных областей технической деятельности. Другие международные организации, правительственные и не правительственные, совместно с ISO и IEC также принимают участие в этой работе. В области информационных технологий, ISO и IEC организован совместный технический комитет, ISO/IEC JTC 1. Основной задачей совместного технического комитета является подготовка Международных Стандартов. Проекты Международных Стандартов принятые совместным техническим комитетом передаются в государственные органы для голосования. Публикация в качестве Международного Стандарта требует одобрения не менее 75 процентов проголосовавших государственных органов. Международные Стандарты проектируются в соответствии с правилами, установленными Директивами ISO/IEC.

### Германский стандарт BSI

В отличие от ISO 17799 германское «Руководство по защите информационных технологий для базового уровня защищенности» посвящено детальному рассмотрению частных вопросов управления информационной безопасностью компании.

В германском стандарте BSI представлены:

* общая методика управления информационной безопасностью (организация менеджмента в области информационной безопасности, методология использования руководства);
* описания компонентов современных ИТ;
* описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса);
* характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны);
* характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение);
* характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell NetWare, сети UNIX и Windows).
* характеристика активного и пассивного телекоммуникационного оборудования ведущих поставщиков, например Cisco Systems;
* подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).
* Вопросы защиты приведенных информационных активов компании рассматриваются по определенному сценарию: общее описание информационного актива компании — возможные угрозы и уязвимости безопасности — возможные меры и средства контроля и защиты.

**Стандарты и рекомендации Банка России в области информационной безопасности**

Центральный Банк РФ проводит большую работу по созданию системы стандартов и рекомендаций, а также методики проверки организаций банковской системы на соответствие их требованиям.

Приняты:

**СТО БР ИББС – 1.0 Общие положения**

**СТО БР ИББС – 1.1 Аудит информационной безопасности**

**СТО БР ИББС – 1.2 Методика оценки соответствия**

Готовятся

**СТО БР ИББС – 0.0 Классификатор**

**СТО БР ИББС – 0.1 Термины и определения**

**РС БР ИББС – 2.0 Документы по обеспечению информационной безопасности**

**РС БР ИББС – 2.1 Руководство по самооценке**

**РС БР ИББС – 2.2 Методика классификации активов**

**РС БР ИББС – 2.3 Методика оценки рисков**

При этом периодически пересматривается

**СТО БР ИББС – 1.0 Общие положения**

Комплекс стандартов Банка России СТО БР ИББС «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» состоит из базового стандарта СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской федерации. Общие положения» (далее – Стандарт) и развивающей и обеспечивающей его группы стандартов и рекомендаций в области стандартизации.

Стандарт основывается на риск - ориентированном подходе, суть которого заключается в том, что деятельность организации БС РФ подвержена рискам, так как на бизнес-процессы организации БС РФ и вовлеченные в них активы могут воздействовать различного рода угрозы. В случае наличия уязвимостей в системе контрмер бизнеса (в это понятие входит, в том числе, и меры обеспечения ИБ организации), а также при наличии определенных условий (факторов риска), реализация угрозы приводит к возникновению инцидента, ведущего к возникновению ущерба для организации БС РФ. Понятие «риск» выступает в этом случае как индикатор угрозы для организации БС РФ и как мера, учитывающая вероятность реализации угрозы (возникновения инцидента) и величину ущерба, являющегося следствием реализации угрозы (возникновения инцидента).

В соответствии с риск- ориентированным подходом в организации БС РФ необходимо реализовать процессы руководства и управления в отношении риска (управление риском), направленные на минимизацию риска или снижение риска до допустимого уровня. Управление риском включает в себя определение допустимого (приемлемого) уровня риска, оценку риска (включая сравнение полученного риска с допустимым) и обработку риска (процесс выбора и осуществления защитных мер, снижающих риски ИБ до приемлемого уровня, или мер по переносу, принятию или уклонению от риска). С целью снижения рисков организация предпринимает комплекс контрмер различного характера (организационных, технических и др.). Необходимо учитывать тот факт, что понизить риски можно лишь до определенного остаточного уровня. Оставшаяся (остаточная) часть риска, определяемая факторами среды деятельности организации БС РФ, на которые организация не в силах влиять, должна быть признана приемлемой и принята, либо отклонена. В этом случае от риска следует либо уклониться (например, изменить среду деятельности), либо перенести на кого-нибудь (например, застраховать).

Риски нарушения ИБ выражаются в возможности потери состояния защищенности интересов (целей) организации БС РФ в информационной сфере и возникновения ущерба бизнесу организации БС РФ или убытков. Потеря состояния защищенности интересов (целей) организации БС РФ в информационной сфере заключается в утрате свойств конфиденциальности, целостности или доступности информационных активов, утрате параметров или доступности сервисов инфраструктуры организации БС РФ.

С целью снижения рисков нарушения ИБ и управления ими (то есть для реализации и поддержания требуемого уровня ИБ) необходимо разработать, реализовать, поддерживать (изучать и анализировать с целью выявления уязвимостей) и совершенствовать (устранять уязвимости и повышать эффективность) систему обеспечения ИБ организации БС РФ.

Система обеспечения ИБ организации БС РФ (СОИБ) представляет собой совокупность системы ИБ и системы менеджмента ИБ организации БС РФ.

Система ИБ организации БС РФ (СИБ) представляет собой совокупность защитных мер, реализующих обеспечение ИБ организации БС РФ, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система менеджмента ИБ (СМИБ) организации БС РФ представляет собой совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов.

Для реализации и поддержания ИБ в организации БС РФ необходима реализация четырех групп процессов:

* планирование СОИБ организации БС РФ (планирование);
* реализация СОИБ организации БС РФ (реализация);
* мониторинг и анализ СОИБ организации БС РФ (проверка);
* поддержка и улучшение СОИБ организации БС РФ (совершенствование).

Указанные группы процессов составляют СМИБ организации БС РФ.

Организация и выполнение процессов СМИБ необходимы, в том числе, для обеспечения уверенности в том, что хороший практический опыт организации БС РФ документируется, становится обязательным к применению, а СОИБ совершенствуется. При этом необходимо обеспечить реализацию всех групп процессов СМИБ. Рис. иллюстрирует взаимосвязь СИБ, СМИБ и СОИБ организации БС РФ.

***СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

***СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

**Реализация**

**СИБ**

**Планирование**

**СИБ**

**Совершенствование**

**СИБ**

**Проверка**

**СИБ**

***СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

**Рис. СОИБ организации БС РФ**

СОИБ должна быть определена, спланирована и регламентирована в организации БС РФ. Основой для этого являются требования законодательства Российской Федерации, нормативные правовые акты Банка России, контрактные требования организации БС РФ, а также условия ведения бизнеса, выраженные на основе идентификации активов организации БС РФ, и построения модели нарушителей и угроз.

Основные принципы, подходы и требования к построению модели угроз и нарушителей содержатся в седьмом разделе Стандарта.

Требования к СИБ и СМИБ организации БС РФ содержатся, соответственно, в восьмом и девятом разделах Стандарта. Однако, учитывая риск -ориентированный подход, используемый в Стандарте, выбор конкретных методов, мер и средств обеспечения ИБ остается за организацией БС РФ и ее руководством.

Даже правильно выстроенные процессы и используемые защитные меры в силу объективных причин со временем имеют тенденцию к ослаблению своей эффективности. Это неминуемо ведет к деградации СОИБ и возрастанию рисков нарушения ИБ.

Для того чтобы избежать деградации СОИБ и обеспечить требуемый уровень ИБ организации БС РФ Стандартом определены требования проверки и оценки СОИБ, которые проводятся путем выполнения следующих процессов: мониторинга и контроля защитных мер, самооценки ИБ, внешнего аудита ИБ, анализа функционирования СОИБ (в том числе со стороны руководства). Указанные процессы являются частью группы процессов «проверка» СМИБ и описаны в десятом разделе Стандарта.

Для поддержания СОИБ на должном уровне в качестве оперативной меры Стандартом определено требование проведения мониторинга СОИБ и контроля защитных мер. В результате выполнения этих процессов может быть выработан сигнал опасности для деятельности организации БС РФ, если произошел инцидент ИБ или выявлены новые угрозы ИБ, уязвимости СОИБ, факторы рисков, требующие введения превентивных мер. В случае возникновения инцидента ИБ должен быть использован дополнительный (специально разработанный) план действий, позволяющий свести к минимуму возможные потери и восстановить СОИБ. Кроме того, результаты выполнения процессов мониторинга и контроля защитных используются для анализа СОИБ, в том числе со стороны руководства.

Для оценки информационной безопасности и выявления признаков деградации СОИБ, Стандартом определено требование проведения самооценки ИБ, а также регулярного внешнего аудита ИБ. При проведении аудита и самооценки ИБ необходимо руководствоваться едиными правилами и подходами и использовать стандартные процедуры. Это позволяет обеспечить точность, повторяемость и сопоставимость результатов, а, следовательно, обеспечить доверие к результатам оценки. Для формирования системы оценки требованиям стандарта СТО БР ИББС-1.0 разработаны стандарты СТО БР ИББС-1.1, СТО БР ИББС-1.2 и рекомендации в области стандартизации РС БР ИББС-2.1.

Стандарт **СТО БР ИББС-1.1** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» устанавливает основные принципы проведения аудита ИБ и требования к процедуре аудита ИБ.

Рекомендации в области стандартизации РС БР ИББС-2.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» устанавливает порядок проведения самооценки ИБ организаций БС РФ.

Стандарт **СТО БР ИББС-1.2** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» устанавливает способы определения степени выполнения требований СТО БР ИББС-1.0, а также итогового уровня соответствия ИБ требованиям СТО БР ИББС-1.0 при проведении аудита (оценки соответствия) ИБ и самооценки ИБ.

Результаты мониторинга, контроля защитных мер, оценки ИБ (самооценки и аудита ИБ) используются при проведении анализа СОИБ (в том числе со стороны руководства).

Анализ СОИБ позволяет выявлять новые угрозы ИБ и факторы рисков ИБ, уязвимости СОИБ. Результаты анализа СОИБ используются для управления рисками ИБ, для принятия решений по тактическим и стратегическим улучшениям СОИБ, по повышению эффективности СОИБ (совершенствование СОИБ организации БС РФ).

Согласно Стандарту, для обеспечения согласованности, целенаправленности, планомерности деятельности по обеспечению ИБ эта деятельность должна быть документирована. Разработку и коррекцию внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в организации БС РФ рекомендуется проводить с учетом рекомендаций по стандартизации Банка России **РС БР ИББС– 2.0** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0», которые определяют состав и структуру документов, а также процессы менеджмента документов по обеспечению ИБ организации БС РФ.

Комплекс стандартов Банка России является концептуальной и методологической основой для обеспечения и поддержания уровня ИБ, необходимого для достижения целей деятельности организации БС РФ и адекватного потребностям и условиям ведения бизнеса организации БС РФ. В настоящее время комплекс стандартов Банка России активно развивается. Готовятся к выходу третья редакция стандарта СТО БР ИББС-1.0 и вторая редакция СТО БР ИББС-1.2, стандарт по терминологии, а также рекомендации по стандартизации, содержащие методику оценки рисков ИБ и методику классификации активов организации БС РФ.

### Стандарты информационной безопасности в Интернете

В Интернете уже давно существует ряд комитетов, в основном из организаций-добровольцев, которые осторожно проводят предлагаемые технологии через процесс стандартизации. Эти комитеты, составляющие основную часть рабочей группы инженеров Интернета IETF (Internet Engineering Task Force) провели стандартизацию нескольких важных протоколов, ускоряя их внедрение в Интернете. Непосредственными результатами усилий IETF являются такие протоколы, как семейство TCP/IP для передачи данных, SMTP (Simple Mail Transport Protocol) и POP (Post Office Protocol) для электронной почты, а также SNMP (Simple Network Management Protocol) для управления сетью.

Фактическая разработка новых стандартов и протоколов для Интернета выполняется рабочими группами, создаваемыми по разрешению группы IETF. Членство в рабочей группе является добровольным; участвовать может любая заинтересованная организация. При разработке спецификации рабочая группа создает документ под названием «Проект стандарта для Интернета» (Internet draft) и размещает его в Интернете для всеобщего доступа. Этот документ может оставаться проектом до шести месяцев, и заинтересованные стороны могут рецензировать и комментировать его. В течение этого времени группа IESG может одобрить публикацию проекта в виде документа RFC (Request for Comment — запрос комментариев). Если проект не приобретает статуса документа RFC в течение шестимесячного периода, он теряет также статус проекта стандарта для Интернета. Однако впоследствии рабочая группа может опубликовать переработанную версию проекта.

Группа IETF публикует документы RFC с одобрения группы IEsG. Документы RFC представляют собой рабочие записи сообщества исследователей и разработчиков Интернета. Документ этой серии может быть чем угодно, от доклада о собрании до спецификации стандарта.

В Интернете популярны протоколы безопасной передачи данных, а именно SSL, SET, IPSec. Перечисленные протоколы появились в Интернете сравнительно недавно как необходимость защиты ценной информации и сразу стали стандартами де-факто.

**Протокол SSL** (Secure Socket Layer) — популярный сетевой протокол с шифрованием данных для безопасной передачи по сети. Он позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи. Протокол SSL обеспечивает защиту данных между сервисными протоколами (такими как HTTP, FTP и др.) и транспортными протоколами (TCP/IP) с помощью современной криптографии. Протокол SSL подробно рассмотрен в главе 11.

**Протокол SET** (Security Electronics Transaction) — перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через сеть Интернет. Протокол SET основан на использовании цифровых сертификатов по стандарту Х.509.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и Visa при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя защищенный механизм выполнения платежей.

SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карточек в Интернете. SET обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения, шифрование ценных и уязвимых данных. Поэтому SET более правильно можно назвать стандартной технологией или системой протоколов выполнения безопасных платежей с использованием пластиковых карт через Интернет. SET позволяет потребителям и продавцам подтверждать подлинность всех участников сделки, происходящей в Интернете, с помощью криптографии, в том числе применяя цифровые сертификаты.

SET обеспечивает следующие специальные требования защиты операций электронной коммерции:

* секретность данных оплаты и конфиденциальность информации заказа, переданной наряду с данными об оплате;
* сохранение целостности данных платежей. Целостность информации платежей обеспечивается с помощью цифровой подписи;
* специальную криптографию с открытым ключом для проведения аутентификации;
* аутентификацию держателя по кредитной карточке. Она обеспечивается применением цифровой подписи и сертификатов держателя карт;
* аутентификацию продавца и его возможности принимать платежи по пластиковым карточкам с применением цифровой подписи и сертификатов продавца;
* аутентификацию того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым карточкам через связь с процессинговой карточной системой. Аутентификация банка продавца обеспечивается использованием цифровой подписи и сертификатов банка продавца;
* готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
* безопасность передачи данных посредством преимущественного использования криптографии.

Основное преимущество SET по сравнению с другими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарт Х509), которые ассоциируют держателя карты, продавца и банк продавца с банковскими учреждениями платежных систем Visa и Mastercard. Кроме того, SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами и интегрируется с существующими системами.

**Протокол IPSec.** Спецификация IPSec входит в стандарт IP v.6 и является дополнительной по отношению к текущей версии протоколов TCP/IP. Она разработана Рабочей группой IP Security IETF. В настоящее время IPSec включает 3 алгоритмо-независимых базовых спецификации, представляющих соответствующие RFC-стандарты. Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и защи­щает информацию на основе сквозного шифрования: независимо от работающего приложения при этом шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете виртуальные частные сети. Протокол IPSec подробно рассмотрен в гл. 12.

**Инфраструктура управления открытыми ключами PKI** (Public Key Infrastructure) предназначена для защищенного управления криптографическими ключами электронного документооборота, основанного на применении криптографии с открытыми ключами. Эта инфраструктура подразумевает использование цифровых сертификатов, удовлетворяющих рекомендациям международного стандарта Х.509 и развернутой сети центров сертификации, обеспечивающих выдачу и сопровождение цифровых сертификатов для всех участников электронного обмена документами.

Конечно, в этом разделе представлено только несколько самых известных стандартов. Общее число их огромно. Даже для банковской сферы их очень много. В стандарте ISO TR 17944-2002 была сделана попытка их разбить на некоторые классы и перечислить. Изучить их все – сложнейшая задача.

**Раздел 2. Угрозы информационной безопасности.**

На протяжении всего периода регулярного использования вычислительной техники для решения практических задач предпринимались попытки классифицировать источники угроз безопасности информации и сами угрозы с целью дальнейшей стандартизации средств и методов, применяемых для защиты информации.

*ГОСТ "Защита информации. Основные термины и определения"* вводит понятие ***информационной безопасности*** как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

***Угроза*** – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Соответственно ***угрозой информационной безопасности*** называется потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или компоненты АИС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

***Атака*** — попытка реализации угрозы.

***Нарушение*** — реализация угрозы.

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется ***окном опасности***, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Определение, анализ и классификация возможных угроз безопасности АИС является одним из важнейших аспектов проблемы обеспечения ее безопасности. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты.

Рассмотрение наиболее распространенных угроз, которым подвержены современные информационные системы дает представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Кроме выявления возможных угроз, должен быть проведен их анализ на основе классификационных признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. При этом угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

# Уязвимости.

В компьютерной безопасности термин **«уязвимость»** (англ. vulnerability) **используется для обозначения недостатка в системе, используя который внешний злоумышленник, может намеренно нарушить её целостность и вызвать неправильную работу.** Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ, скриптовых и SQL-инъекций. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты.

В приведенных ниже списках даны примеры уязвимостей в различных сферах безопасности, включая примеры угроз, которые могут использовать эти уязвимости. Эти списки могут быть полезными во время оценки уязвимостей. Следует подчеркнуть, что в некоторых случаях эти уязвимости могут использоваться и другими угрозами.

**1. Внешняя среда и инфраструктура**

* Отсутствие физической защиты здания, дверей и окон (может быть использовано, например, угрозой хищения).
* Неадекватное или небрежное использование физического управления доступом к зданиям и помещениям (может быть использовано, например, угрозой намеренного повреждения).
* Нестабильная электрическая сеть (может быть использована, например, угрозой колебаний напряжения).
* Размещение в местности, предрасположенной к наводнениям (может быть использовано, например, угрозой затопления).

**2. Аппаратные средства**

* Отсутствие программ периодической замены (может быть использовано, например, угрозой ухудшения состояния носителей данных).
* Чувствительность к колебаниям напряжения (может быть использована, например, угрозой колебаний напряжения).
* Чувствительность к колебаниям температуры (может быть использована, например, угрозой экстремальных показателей температуры).
* Чувствительность к влажности, пыли, загрязнению (может быть использована, например, угрозой пылеобразования).
* Чувствительность к электромагнитному излучению (может быть использована, например, угрозой электромагнитного излучения).
* Недостаточное техническое обслуживание/неправильная установка носителей данных (может быть использовано, например, угрозой ошибки технического обслуживания).
* Отсутствие эффективного контроля изменений конфигурации (может быть использовано, например, угрозой ошибок операционного персонала).

**3. Программные средства**

* Нечеткие или неполные спецификации для разработчиков (могут быть использованы, например, угрозой сбоя программы).
* Отсутствующее или недостаточное тестирование программных средств (может быть использовано, например, угрозой использования программных средств неуполномоченными пользователями).
* Сложный пользовательский интерфейс (может быть использован, например, угрозой ошибок операционного персонала).
* Отсутствие механизмов идентификации и аутентификации, таких как аутентификация пользователей (может быть использовано, например, угрозой имитации личности пользователя).
* Отсутствие контрольного журнала (может быть использовано, например, угрозой использования программных средств несанкционированным образом).
* Широко известные дефекты программных средств (могут быть использованы, например, угрозой использования программных средств неуполномоченными пользователями).
* Незащищенные таблицы паролей (могут быть использованы, например, угрозой имитации личности пользователя).
* Плохой менеджмент паролей (легко отгадываемые пароли, хранение паролей в незашифрованном виде, недостаточная частота смены паролей) (может быть использован, например, угрозой имитации личности пользователя).
* Неверное распределение прав доступа (может быть использовано, например, угрозой использования программных средств несанкционированным образом).
* Неконтролируемая загрузка и использование программных средств (может быть использована, например, угрозой вредоносного программного обеспечения).
* Отсутствие «конца сеанса», покидая рабочую станцию (может быть использовано, например, угрозой использования программных средств неуполномоченными пользователями).
* Отсутствие эффективного контроля изменений (может быть использовано, например, угрозой сбоя программы).
* Отсутствие документации (может быть использовано, например, угрозой ошибок операционного персонала).
* Отсутствие резервных копий (может быть использовано, например, угрозой вредоносного программного обеспечения или угрозой пожара).
* Списание или повторное использование носителей данных без надлежащего стирания (может быть использовано, например, угрозой использования программных средств неуполномоченными пользователями).
* Активированные ненужные службы (могут быть использованы, например, угрозой использования несанкционированного программного обеспечения).
* Недоработанное или новое программное обеспечение (может быть использовано, например, угрозой некомпетентного или неадекватного тестирования).
* Широко распределенное программное обеспечение (может быть использовано, например, угрозой потери целостности в процессе распределения).

**4. Система связи**

* Незащищенные линии связи (могут быть использованы, например, угрозой подслушивания).
* Плохая разводка кабелей (может быть использована, например, угрозой проникновения в систему связи).
* Отсутствие идентификации и аутентификации отправителя и получателя (может быть использовано, например, угрозой имитации личности пользователя).
* Коммутируемые линии (могут быть использованы, например, угрозой получения сетевого доступа неуполномоченными пользователями).
* Незащищенный значимый трафик (может быть использован, например, угрозой подслушивания).
* Неадекватный сетевой менеджмент (устойчивость маршрутизации) (может быть использован, например, угрозой перегрузки трафика).
* Незащищенные соединения сети общего пользования (могут быть использованы, например, угрозой использования программных средств неуполномоченными пользователями)
* Ненадежная сетевая архитектура (может быть использована, например, угрозой вторжения).

**5. Документы**

* Незащищенное хранение (может быть использовано, например, угрозой хищения). Беззаботность при устранении (может быть использована, например, угрозой хищения).
* Неконтролируемое копирование (может быть использовано, например, угрозой хищения).

**6. Персонал**

* Отсутствие персонала (может быть использовано, например, угрозой нехватки персонала).
* Безнадзорная работа внешнего персонала или персонала, занимающегося уборкой (может быть использована, например, угрозой хищения).
* Недостаточное обучение по безопасности (может быть использовано, например, угрозой ошибок операционного персонала).
* Отсутствие осознания безопасности (может быть использовано, например, угрозой ошибок пользователей).
* Ненадлежащее использование программных и аппаратных средств (может быть использовано, например, угрозой ошибок операционного персонала).
* Отсутствие механизмов мониторинга (может быть использовано, например, угрозой использования программных средств несанкционированным образом).
* Отсутствие политик по правильному использованию телекоммуникационной среды и обмена сообщениями (может быть использовано, например, угрозой использования сетевых средств несанкционированным образом).
* Неадекватные процедуры набора персонала (могут быть использованы, например, угрозой намеренного повреждения).

**7. Процедурные**

* Отсутствие санкционирования средств обработки информации (может быть использовано, например, угрозой намеренного повреждения).
* Отсутствие формального процесса санкционирования общедоступной информации (может быть использовано, например, угрозой ввода искаженных данных).
* Отсутствие формального процесса проверки прав доступа (надзора) (может быть использовано, например, угрозой несанкционированного доступа).
* Отсутствие формальной политики по использованию портативных компьютеров (может быть использовано, например, угрозой хищения).
* Отсутствие формальной процедуры контроля документации системы менеджмента информационной безопасности (может быть использовано, например, угрозой ввода искаженных данных).
* Отсутствие формальной процедуры надзора за записями системы менеджмента информационной безопасности (может быть использовано, например, угрозой ввода искаженных данных).
* Отсутствие формальной процедуры регистрации и отмены регистрации пользователей (может быть использовано, например, угрозой несанкционированного доступа).
* Отсутствие контроля за резервными активами (может быть использовано, например, угрозой хищения).
* Отсутствующее или неудовлетворительное соглашение об уровне сервиса (может быть использовано, например, угрозой ошибок технического обслуживания).
* Отсутствующая или недостаточная политика «чистого стола и пустого экрана» (может быть использована, например, угрозой хищения информации).
* Отсутствующие или недостаточные положения (касающиеся безопасности) в договорах с клиентами и/или третьими сторонами (могут быть использованы, например, угрозой несанкционированного доступа).
* Отсутствующие или недостаточные положения (касающиеся безопасности) в договорах со служащими (могут быть использованы, например, угрозой мошенничества и хищения).
* Отсутствие планов обеспечения деловой непрерывности (может быть использовано, например, угрозой технической неисправности).
* Отсутствие надлежащего распределения обязанностей по обеспечению информационной безопасности (может быть использовано, например, угрозой отрицания).
* Отсутствие политики по использованию электронной почты (может быть использовано, например, угрозой неправильной маршрутизации сообщений).
* Отсутствие процедур идентификации и оценки риска (может быть использовано, например, угрозой несанкционированного доступа к системе).
* Отсутствие процедур обращения с секретной информацией (может быть использовано, например, угрозой ошибок пользователей).
* Отсутствие процедур обеспечения соблюдения прав на
* интеллектуальную собственность (может быть использовано, например, угрозой хищения информации).
* Отсутствие процедур сообщения о слабых местах безопасности (может быть использовано, например, угрозой использования сетевых средств несанкционированным образом).
* Отсутствие процедур введения программного обеспечения в действующие системы (может быть использовано, например, угрозой ошибок операционного персонала).
* Отсутствие процедуры контроля изменений (может быть использовано, например, угрозой ошибки технического обслуживания).
* Отсутствие процедуры мониторинга средств обработки информации (может быть использовано, например, угрозой несанкционированного доступа).
* Отсутствие регулярных аудитов (надзора) (может быть использовано, например, угрозой несанкционированного доступа).
* Отсутствие регулярных проверок, проводимых руководством (может быть использовано, например, угрозой злоупотребления ресурсами).
* Отсутствие установленных механизмов мониторинга нарушений безопасности (может быть использовано, например, угрозой умышленного повреждения).
* Отсутствие обязанностей по обеспечению информационной безопасности в перечнях служебных обязанностей (может быть использовано, например, угрозой ошибок пользователей).
* Отсутствие зафиксированных в журнале регистрации администратора и оператора сообщений об ошибках (может быть использовано, например, угрозой использования программных средств несанкционированным образом).
* Отсутствие записей в журнале регистрации администратора и оператора (может быть использовано, например, угрозой ошибок операционного персонала).
* Отсутствие оговоренного дисциплинарного процесса в случае инцидента безопасности (может быть использовано, например, угрозой хищения информации).

**8. Обычные уязвимости обработки бизнес-приложений**

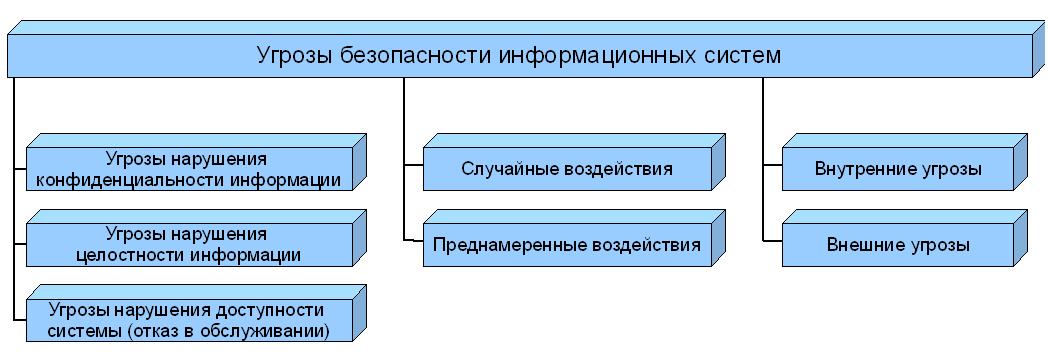
* Неверная установка параметров (может быть использована, например, угрозой ошибок пользователей).
* Применение прикладных программ к неверным данным с точки зрения времени (может быть использовано, например, угрозой недоступности данных).
* Неспособность создания административных отчетов (может быть использована, например, угрозой несанкционированного доступа).
* Неверные даты (могут быть использованы, например, угрозой ошибок пользователей).

**9. Общеприменимые уязвимости**

* Единичная точка сбоя (может быть использована, например, угрозой сбоя услуг связи).
* Неадекватное реагирование технического обслуживания (может быть использовано, например, угрозой сбоев аппаратных средств).
* Неправильно разработанные, несоответствующим образом выбранные или плохо управляемые защитные меры (могут быть использованы, например, угрозой проникновения в систему связи).

# Классификация угроз информационной безопасности

***Классификацию угроз ИБ можно выполнить по нескольким критериям:***



1. ***По аспекту ИБ***: угрозы конфиденциальности, угрозы целостности, угрозы доступности. Дополнительно можно выделить угрозы аутентичности и апеллируемости.

2. ***По компонентам АИС, на которые нацелена угроза***: данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура).

3. ***По расположению источника угроз***: внутри или вне рассматриваемой АИС. Угрозы со стороны инсайдеров являются наиболее опасными.

4. ***По природе возникновения:*** естественные (объективные) и искусственные (субъективные).

***Естественные угрозы*** — это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

***Искусственные угрозы*** — угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить ***непреднамеренные*** (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п., и ***преднамеренные*** (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

***5. По непосредственному источнику угроз.***

5.1. ***Угрозы, непосредственным источником которых является природная среда*** (стихийные бедствия, магнитные бури, радиоактивное излучение и т.п.).

5***.2. Угрозы, источником которых является человек:***

* внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
* вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
* угроза несанкционированного копирования секретных данных пользователем АС;
* разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

***5.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства:***

* запуск технологических программ, способных при некомпетентном пользовании вызывать потерю работоспособности системы (зависания) или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.);
* возникновение отказа в работе операционной системы.

***5.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства:***

* нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
* заражение компьютера вирусами с деструктивными функциями.

***6. По положению источника угроз.***

***6.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС:***

* перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.);
* перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
* дистанционная фото- и видеосъемка.

***6.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС:***

* хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
* отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.д.);
* применение подслушивающих устройств.

***6.3. Угрозы, источник которых имеет доступ к периферийным устройства АС(терминалам).***

***6.4. Угрозы, источник которых расположен в АС:***

* проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации;
* некорректное использование ресурсов АС.

***7. По степени зависимости от активности АС.***

***7.1. Угрозы, которые могут проявляться независимо от активности АС:***

* вскрытие шифров криптозащиты информации;
* хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).

***7.2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных*** (например, угрозы выполнения и распространения программных вирусов).

***8. По степени воздействия на АС.***

***8.1. Пассивные угрозы,*** которые при реализации ничего не меняют в структуре и содержании АС(угроза копирования секретных данных)***.***

***8.2. Активные угрозы***, которые при воздействии вносят изменения в структуру и содержание АС:

* внедрение аппаратных спецвложений, программных "закладок" и "вирусов" ("троянских коней" и "жучков"), т.е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
* действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
* угроза умышленной модификации информации.

***9. По этапам доступа пользователей или программ к ресурсам АС.***

***9.1. Угрозы, которые могут проявляться на этапе доступа к ресурсам АС***(например, угрозы несанкционированного доступа в АС).

***9.2. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС***(например, угрозы несанкционированного или некорректного использования ресурсов АС).

***10. По способу доступа к ресурсам АС.***

***10.1. Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС:***

* незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");
* несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.

***10.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС:***

* вход в систему в обход средств защиты (загрузка посторонней опера ционной системы со сменных магнитных носителей и т.п.);
* угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.

***11. По текущему месту расположения информации, хранимой и обрабатываемой в АС.***

***11.1. Угрозы доступа к информации на внешних запоминающих устройства***(например, угроза несанкционированного копирования секретной информации с жесткого диска).

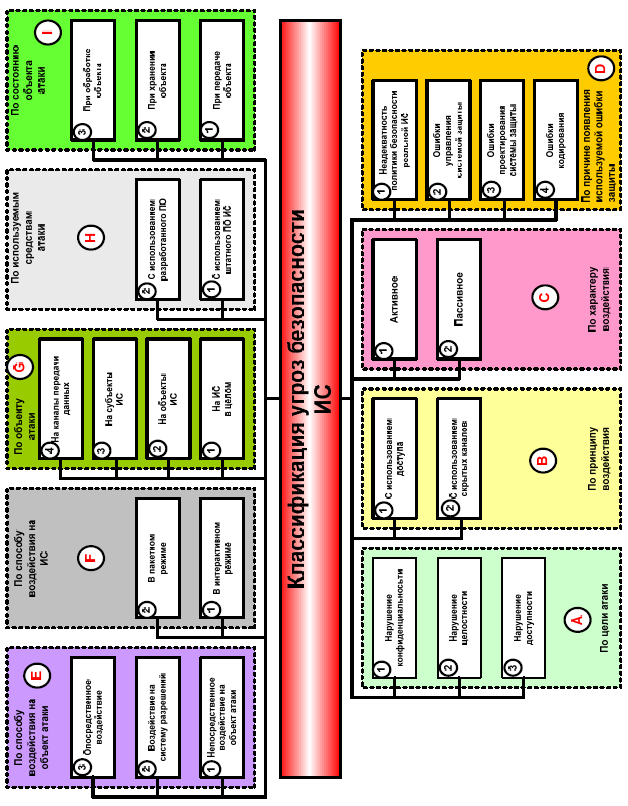
***11.2. Угрозы доступа к информации в оперативной памяти:***

* чтение остаточной информации из оперативной памяти;
* чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования;
* угроза доступа к системной области оперативной памяти со сторон прикладных программ.

***11.3. Угрозы доступа к информации, циркулирующей в линиях связи:***

* незаконное подключение к линиям связи с целью работы во время пауз в действиях законного пользователя от его имени с вводом ложных сообщений или модификацией передаваемых сообщений;
* незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;
* перехват всего потока данных с целью дальнейшего анализа не в реальном масштабе времени.

***11.4. Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере (***например, угроза записи отображаемой информации на скрытую видеокамеру).



***Угроза доступности (отказа служб)***возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным - запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

***Угроза нарушения целостности*** включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую, в том числе и несанкционированное изменение информации при случайных ошибках программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, периодическая запланированная коррекция некоторой базы данных).

***Угроза нарушения конфиденциальности*** заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин "утечка".

На современном этапе развития информационных технологий под системы или функции защиты являются неотъемлемой частью комплекса по обработке информации. Информация не представляется "в чистом виде", на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому чтобы угрожать, атакующая сторона должна преодолеть эту систему. Однако не существует абсолютно стойкой системы защиты, вопрос лишь во времени и средствах, требующихся на ее преодоление. Исходя из данных условий, примем следующую модель: ***защита информационной системы считается преодоленной, если в ходе ее исследования определены все уязвимости системы.*** Поскольку преодоление защиты также представляет собой угрозу, для защищенных систем будем рассматривать ее четвертый вид-***угрозу раскрытия параметров АС,*** включающей в себя систему защиты. С точки зрения практики любое проводимое мероприятие предваряется этапом разведки, в ходе которого определяются основные параметры системы, её характеристики, в результате чего уточняется поставленная задача и выбираются оптимальные технические средства.

Угрозу раскрытия можно рассматривать как опосредованную. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализоваться первичным или непосредственным угрозам, перечисленным выше.

Такая классификация (поддерживается подавляющим большинством специалистов) предусматривает подразделение угроз на **информационные, программно-математические, физические и организационные.**

**Информационные угрозы** реализуются в виде:

- нарушения адресности и своевременности информационного обмена;

- противозаконного сбора и использования информации;

- осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

- хищения информационных ресурсов из банков и баз данных;

- нарушения технологии обработки информации.

**Программно-математические угрозы** реализуются в виде:

- внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;

- разработки и распространения программ, нарушающих нормальное функционирование информационных систем или их систем защиты

информации.

**Физические угрозы** реализуются в виде:

- уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;

- уничтожения, повреждения, разрушения или хищения машинных и других носителей информации;

- хищения программных или аппаратных ключей и средств криптографической защиты информации;

- перехвата информации в технических каналах связи и телекоммуникационных системах;

- внедрения электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения;

- перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;

- воздействия на парольно-ключевые системы защиты средств обработки и передачи информации.

**Организационные угрозы** реализуются в виде:

- невыполнения требований законодательства в информационной сфере;

- противоправной закупки несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации

и связи.

# Предпосылки появления угроз.

Существует две возможные разновидности предпосылок: **объективные** (количественная или качественная недостаточность элементов системы) и **субъективные** (деятельность разведорганов иностранных государств, промышленный шпионаж, деятельность уголовных элементов, действия недобросовестных сотрудников системы).

Перечисленные разновидности предпосылок интерпретируются следующим образом:

***количественная недостаточность*** – физическая нехватка одного или нескольких элементов системы, вызывающая нарушения технологического процесса обработки данных и/или перегрузку имеющихся элементов;

***качественная недостаточность*** – несовершенство конструкции (организации) элементов системы, в силу чего могут появляться возможности случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

***деятельность разведорганов иностранных государств*** – специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами.

К основным видам разведки относятся **агентурная** (несанкционированная деятельность профессиональных разведчиков, завербованных агентов и так называемых «доброжелателей», «инициативников») и **техническая**, включающая **радиоразведку** (перехват радиоэлектронными средствами информации, циркулирующей в телекоммуникационных каналах), **радиотехническую разведку** (регистрацию спецсредствами электромагнитных излучений технических систем) и **космическую разведку** (использование космических кораблей и искусственных спутников Земли для наблюдения за территорией, ее фотографирования, регистрации радиосигналов и получения полезной информации любыми другими доступными способами);

**промышленный шпионаж** – негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной ее утечки или хищения, с целью создания для себя благоприятных условий и получения максимальных выгод (недобросовестная конкуренция);

**злоумышленные действия уголовных элементов** – хищение информации или компьютерных программ в целях наживы;

**действия недобросовестных сотрудников** – хищение (копирование) или уничтожение информационных массивов и/или программ по эгоистическим или корыстным мотивам, а также в результате несоблюдения установленного порядка работы с информацией.

# Источники угроз.

Под источником угроз понимается непосредственный ее генератор или носитель.

Таким источником могут быть люди, технические средства, модели (алгоритмы), программы, внешняя среда.

Модели угроз и нарушителей ИБ для организации БС РФ рассматриваются в стандарте СТО БР ИББС 0.1-2006 (Раздел 7). Встандарте выделено следующее.

***Модели угроз и нарушителей должны быть основным инструментом менеджмента организации при развертывании, поддержании и совершенствовании системы обеспечения ИБ организации.***

Деятельность организации БС РФ поддерживается входящей в ее состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);

- сетевого (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);

- сетевых приложений и сервисов;

- операционных систем (ОС);

- систем управления базами данных (СУБД);

- банковских технологических процессов и приложений;

- бизнес-процессов организации.

На каждом из уровней угрозы и их источники (в т.ч. злоумышленники), методы и средства защиты и подходы к оценке эффективности являются различными.

Главной целью злоумышленника является получение контроля над активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов, например, путем раскрытия конфиденциальной банковской аналитической информации, более эффективно для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через нижние уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективное по соотношению «затраты/получаемый результат».

Организация должна определить конкретные объекты защиты на каждом из уровней информационной инфраструктуры.

Наиболее актуальные источники угроз **на физическом, сетевом уровнях и уровне сетевых приложений**:

- внешние источники угроз: лица, распространяющие вирусы и другие вредоносные программы, хакеры, фрикеры; и иные лица, осуществляющие несанкционированный доступ (НСД);

- внутренние источники угроз, реализующие угрозы в рамках своихполномочий и за их пределами (персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы сетевых приложений и т.п.);

- комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно.

Наиболее актуальные источники у**гроз на уровнях операционных**

**систем, систем управления базами данных, банковских технологических п**роцессов:

- внутренние, реализующие угрозы в рамках своих полномочий и за их пределами (администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.);

- комбинированные источники угроз: внешние и внутренние, действующие в сговоре.

Наиболее актуальные источники угроз на **уровне бизнес-процессов**:

- внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами (авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.);

- комбинированные источники угроз: внешние (например, конкуренты) и внутренние, действующие в сговоре.

Также необходимо учитывать угрозы, связанные с природными и техногенными катастрофами и террористической деятельностью.

Источники угроз для реализации угрозы используют уязвимости объектов и системы защиты.

Хорошей практикой является разработка моделей угроз и нарушителей ИБ для данной организации.

**Модель угроз ИБ** включает описание источников угрозы, уязвимостей, используемых угрозами, методов и объектов нападений, пригодных для реализации угрозы, типов возможной потери (например, конфиденциальности, целостности, доступности активов), масштабов потенциального ущерба.

Для источников угроз – людей – может быть разработана модель нарушителя ИБ, включающая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, и возможной мотивации их действий.

Степень детализации параметров моделей угроз и нарушителей ИБ может быть различна и определяется реальными потребностями для каждой организации в отдельности.

**В руководящем документе Гостехкомиссии России [РД. Концепция защиты средств вычислительной техники в АС от НСД к информации, 1992]** введено ***понятие модели нарушителя*** в автоматизированной системе обработки данных. В качестве такового рассматривается *субъект, имеющий доступ к работе со штатными средствами АС.* При этом в зависимости от возможностей, предоставляемых нарушителям штатными средствами, угрозы делятся на четыре уровня:

**самый низкий** – возможности запуска задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции обработки информации;

**промежуточный 1** – дополнительно к предыдущему имеются возможности создания и запуска собственных программ с новыми функциями обработки информации;

**промежуточный 2** – дополнительно к предыдущему предполагается наличие возможностей управления функционированием АС, т.е. воздействия на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования;

**самый высокий** – определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав системы собственных технических средств с новыми функциями обработки информации (в этом случае предполагается, что нарушитель является специалистом высшей квалификации, знает все об АС, в том числе и об используемых средствах защиты информации).

Согласно [СТР-К] различают 4 уровня возможностей внутреннего нарушителя, которые увеличиваются от уровня к уровню.

**первый уровень** – возможность запуска программ из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации (пользователь АРМ, пользователь сети);

**второй уровень** – возможность создания и запуска собственных программ с новыми функциями по обработке информации (прикладной программист, разработчик программного обеспечения);

**третий уровень** – возможность получения управления функционированием системы, а также воздействия на базовое программное обеспечение, состав и конфигурацию оборудования (системный программист, администратор сервера (ЛВС), администратор информационной системы (базы данных), разработчик);

**четвертый уровень** – определяется возможностью проектирования, установки и ремонта средств электронно-вычислительной техники, вплоть до включения в их состав собственных технических и программных средств с новыми функциями по обработке информации (администратор информационной системы, администратор сервера (ЛВС), администратор безопасности информации, разработчик системы, разработчик средств защиты информации, обслуживающий АС персонал).

Таблица 1. Основные методы реализации угроз информационной безопасности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Уровень  доступа  к информации  в AC | Угроза  раскрытия  параметров  системы | Угроза  нарушения  конфиденциальности | Угроза  нарушений  целостности | Угроза отказа  служб (отказа  доступа  к информации) |
| Уровень  носителей  информации | Определение  типа и пара-  метров носителей  информации | Хищение (копирование)  носителей информации. Перехват ПЭМИН | Уничтожение  машинных  носителей информации | Выведение  из строя  машинных  носителей информации |
| Уровень  средств  взаимодействия  с носителем | Получение  информации  о программно-  аппаратной  среде. Получение детальной  информации  о функциях,  выполняемых AC  Получение  данных о применяемых системах защиты | Несанкционированный доступ к ресурсам AC Совершение пользователем несанкционированных действий.  Несанкционированное  копирование  программного  обеспечения.  Перехват данных,  передаваемых  по каналам связи | Внесение  пользователем  несанкционированных изменений  в программы и данные.  Установка и использование  Нештатного программного  обеспечения.  Заражение программными  вирусами | Проявление  ошибок  проектирования  и разработки  программно-  аппаратных  компонент AC  Обход механизмов защиты AC |
| Уровень  представления  информации | Определение  способа  представления  информации | Визуальное  наблюдение.  Раскрытие  представления  информации  (дешифрование) | Внесение  искажения  в представление  данных;  уничтожение  данных языка | Искажение  соответствия  синтаксических  и семантических  конструкций |
| Уровень  содержания  информации | Определение  содержания  данных  на качественном уровне | Раскрытие  содержания  информации | Внедрение  дезинформации | Запрет  на использование  информации |

# Неформальная модель нарушителя

***Нарушитель***— лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

***Злоумышленником***будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Для того, чтобы определить вероятные источники угроз информационной безопасности АИС и показатели риска для этих угроз строится ***неформальная модель нарушителя*.** Такая модель отражает потенциальные возможности и знания нарушителя, время и место действия, необходимые усилия и средства для осуществления атаки и т.п. и в идеале должны быть адекватна реальному нарушителю для данной АИС.

Модель нарушителя включает следующие (обоснованные) предположения:

***1. О категориях лиц, к которым может принадлежать нарушитель*:** пользователи системы, обслуживающий персонал, разработчики АИС, сотрудники службы безопасности, руководители — внутренние нарушители; клиенты, посетители, конкуренты, случайные лица — внешние нарушители.

***2. О мотивах нарушителя.***Основными мотивами считаются три: безответственность, самоутверждение или корыстный интерес. В первом случае нарушения вызываются некомпетентностью или небрежностью без наличия злого умысла. Во втором случае нарушитель, преодолевая защиту АИС и получая доступ к системным данным, самоутверждается в собственных глазах или в глазах коллег (такой нарушитель рассматривает свои действия как игру «пользователь — против системы»). Наибольшей опасностью обладает третий тип нарушителя, который целенаправленно преодолевает систему защиты, движимый корыстным интересом.

***3. Об уровне знаний нарушителя:***на уровне пользователя АИС, на уровне администратора АИС, на уровне программиста, на уровне специалиста в области информационной безопасности.

***4. О возможностях нарушителя (используемых методах и средствах):***применяющий только агентурные методы, применяющий только штатные средства доступа к данным (возможно, в несанкционированном режиме), применяющий пассивные средства (возможность перехвата данных), применяющий активные средства (возможность перехвата и модификации данных).

***5. О времени действия:*** во время штатного функционирования АИС, во время простоя АИС, в любое время.

***6. О месте действия:*** без доступа на контролируемую территорию организации, с доступом на контролируемую территорию (но без доступа к техническим средствам), с рабочих мест пользователей, с доступом к базам данных АИС, с доступом к подсистеме защиты АИС.

Неформальная модель нарушителя строится на основе исследования АИС (аппаратных и программных средств) с учетом специфики предметной области и используемой в организации технологии обработки данных.

Поскольку определение конкретных значений характеристик возможных нарушителей — в значительной степени субъективный процесс, обычно модель включает несколько обликов возможного нарушителя, по каждому из которых определяются значения всех приведенные выше характеристик. Наличие неформальной модели нарушителя позволяет выявить причины возможных нарушений информационной безопасности и либо устранить эти причины, либо усовершенствовать систему защиты от данного вида нарушений.

Таблица 2. Модель нарушителя в информационных системах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Группа | Возможности проникновения | | | |
| Запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации | Создание и запуск собственных программ с новыми функциями по обработке информации | Возможность управления функционированием ИС, (воздействие на базовое ПО, на состав и конфигурацию ее оборудования) | Полное и всестороннее воздействие на средства ИС, вплоть до включения в состав ИС своих средств и ПО |
| Начинающий взломщик | + |  |  |  |
| Освоивший основы работы на ПЭВМ и в составе сети | + | + |  |  |
| Классный специалист | + | + | + |  |
| Специалист  высшего  класса | + | + | + | + |



# Способы НСД к информации.

; ***Несанкционированный доступ к источникам конфиденциальной информации*** — это противоправное преднамеренное овладение ею. В лекции рассмотрены способы НСД, обобщенная модель способов НСД к источникам конфиденциальной информации, методы и средства защиты от НСД в сети.

Способ несанкционированного доступа - это совокупность приемов, позволяющих злоумышленнику получить охраняемые сведения конфиденциального характера.

Способами несанкционированного доступа являются:

1. Инициативное сотрудничество.

2. Склонение к сотрудничеству.

3. Выведывание, выпытывание.

4. Подслушивание.

5. Наблюдение.

6. Хищение.

7. Копирование.

8. Подделка (модификация).

9. Уничтожение.

10. Незаконное подключение.

11. Перехват.

12. Негласное ознакомление.

13. Фотографирование.

14. Сбор и аналитическая обработка информации.

***Инициативное сотрудничество*** проявляется в определенных действиях лиц, чем-то неудовлетворенных или остро нуждающихся в средствах к существованию, из числа работающих на предприятии, готовых ради наживы на любые противоправные действия. Наличие такого человека в сфере производства и управления предприятия позволяет злоумышленникам получать необходимые сведения о деятельности фирмы.

***Склонение к сотрудничеству*** — это, как правило, насильственное действие со стороны злоумышленников. Склонение или вербовка может осуществляться путем подкупа, запугивания, шантажа.

***Выведывание, выпытывание*** — это стремление под видом наивных вопросов получить определенные сведения.

***Подслушивание*** — способ ведения разведки и промышленного шпионажа, применяемый агентами, наблюдателями, информаторами, специальными постами подслушивания. Злоумышленники используют для этого специальных людей, сотрудников, современную технику, различные приемы ее применения. Подслушивание может осуществляться непосредственным восприятием акустических колебаний лицом при прямом восприятии речевой информации либо с помощью технических средств.

***Наблюдение*** — способ ведения разведки о состоянии и деятельности противника. Ведется визуально и с помощью оптических приборов. Процесс наблюдения довольно сложен, так как требует значительных затрат сил и средств.

***Хищение*** — умышленное противоправное завладение чужим имуществом, средствами, документами, материалами, информацией. Похищают документы, продукцию, дискеты, ключи, коды, пароли и шифры.

***Копирование*** - копируют документы, содержащие интересующие злоумышленника сведения; информацию, обрабатываемую в АСОД (автоматизированные системы обработки данных); продукцию.

***Подделка*** (модификация, фальсификация) Подделывают доверительные документы, позволяющие получить определенную информацию, письма, счета, бухгалтерскую и финансовую документацию, ключи, пропуска, пароли и т. д.

***Уничтожение.*** В части информации особую опасность представляет ее уничтожение в АСОД, в которой накапливаются на технических носителях огромные объемы сведений различного характера, причем многие из них весьма трудно изготовить в виде немашинных аналогов.

***Незаконное подключение.*** Под незаконным подключением будем понимать контактное или бесконтактное подключение к различным линиям и проводам с целью несанкционированного доступа к информации. Подключение возможно как к проводным линиям телефонной и телеграфной связи, так и к линиям связи иного информационного назначения: линиям передачи данных, соединительным линиям периферийных устройств больших и малых ЭВМ, линиям диспетчерской связи, конференцсвязи, питания, заземления и другими.

***Перехват.*** В практике радиоэлектронной разведки под перехватом понимают получение разведывательной информации за счет приема сигналов электромагнитной энергии пассивными средствами приема, расположенными, как правило, на достаточном расстоянии от источника конфиденциальной информации. Перехвату подвержены переговоры любых систем радиосвязи, переговоры, ведущиеся с подвижных средств телефонной связи (радиотелефон), переговоры внутри помещения посредством бесшнуровых систем учрежденческой связи и другие.

***Негласное ознакомление*** — способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать (открытый документ на столе во время беседы с посетителем, наблюдение экрана ПЭВМ со значительного расстояния в момент работы с закрытой информацией и т. д.). К негласному ознакомлению относится и перлюстрация почтовых отправлений, учрежденческой и личной переписки.

***Фотографирование*** — способ получения видимого изображения на фотоматериале. Особенность способа — документальность, позволяющая при дешифровании фотоснимков по элементам и демаскирующим признакам получить весьма ценные, детальные сведения об объекте наблюдения.

***Сбор и аналитическая обработка*** являются завершающим этапом изучения и обобщения добытой информации с целью получения достоверных и объемлющих сведений по интересующему злоумышленника аспекту деятельности объекта его интересов. Полный объем сведений о деятельности конкурента не может быть получен каким-нибудь одним способом. Чем большими информационными возможностями обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе. На успех может рассчитывать тот, кто быстрее и полнее соберет необходимую информацию, переработает ее и примет правильное решение.

# Каналы несанкционированного получения информации (КНПИ)

***КНПИ*** – это физический канал от источника защищаемой информации к злоумышленнику, по которому возможна утечка охраняемых сведений.

**Классифицируем все возможные каналы несанкционированного** **получения информации (КНПИ)** по двум критериям:

1. необходимости доступа (физического или логического) к элементам АС для реализации того или иного КНПИ

2. зависимости появления КНПИ от состояния АС.

***По первому критерию КНПИ*** могут быть разделены на **не требующие доступа**, т.е. позволяющие получать необходимую информацию дистанционно (например, путем визуального наблюдения через окна помещений АС), и **требующие доступа** в помещения АС.

В свою очередь, КНПИ, воспользоваться которыми можно только получив доступ в помещения АС, делятся на **не оставляющие следы** в АС (например, визуальный просмотр изображений на экранах мониторов или документов на бумажных носителях) и на КНПИ, использование которых **оставляет те или иные следы** (например, хищение документов или машинных носителей информации).

***По второму критерию КНПИ*** делятся на **постоянно существующие** независимо от состояния АС (например, похищать носители информации можно независимо от того, в рабочем состоянии находятся средства АС или нет) и **существующие только в рабочем состоянии** АС (например, побочные электромагнитные излучения и наводки).

**КНПИ 1-го класса** – каналы, проявляющиеся безотносительно к обработке информации и без доступа злоумышленника к элементам системы.

Сюда может быть отнесено подслушивание разговоров, а также провоцирование на разговоры лиц, имеющих отношение к АС, и использование злоумышленником визуальных, оптических и акустических средств.

Данный канал может проявиться и путем хищения носителей информации в момент их нахождения за пределами помещения, где расположена АС.

**КНПИ 2-го класса** – каналы, проявляющиеся в процессе обработки информации без доступа злоумышленника к элементам АС.

Сюда могут быть отнесены электромагнитные излучения различных устройств ЭВМ, аппаратуры и линий связи, паразитные наводки в цепях питания, телефонных сетях, системах теплоснабжения, вентиляции и канализации, шинах заземления, подключение к информационно-вычислительной сети генераторов помех и регистрирующей аппаратуры. К этому же классу может быть отнесен осмотр отходов производства, попадающих за пределы контролируемой зоны.

**КНПИ 3-го класса** – каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АС, но без изменения последних.

К ним относятся всевозможные виды копирования носителей информации и документов, а также хищение производственных отходов.

**КНПИ 4-го класса** – каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АС, но без изменения последних.

Сюда может быть отнесено запоминание и копирование информации в процессе обработки, использование программных ловушек, недостатков языков программирования и операционных систем, а также поражение программного обеспечения вредоносными закладками, маскировка под зарегистрированного пользователя.

**КНПИ 5-го класса** – каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АС и с изменением последних.

Среди этих каналов: подмена и хищение носителей информации и аппаратуры, включение в программы блоков типа «троянский конь», «компьютерный червь» и т.п., чтение остаточной информации, содержащейся в памяти, после выполнения санкционированных запросов.

**КНПИ 6-го класса** – каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АС и с изменением последних.

Сюда может быть отнесено незаконное подключение к аппаратуре и линиям связи, а также снятие информации на шинах питания различных элементов АС.

# ВТСС. ОТСС. Функциональное назначение.

**Объект защиты информации** - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации

К объектам защиты относятся:

Информационные активы;

ЗП(Защищаемые(выделенные) помещения);

ОТСС (Основные технические средства и системы);

ВТСС (Вспомогательные технические средства и системы).

До середины 20 века существовало следующее определение информации:

**Информация** – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т.д.)

Понятие «сообщение» часто определяется как «кодированный эквивалент события, зафиксированный источником информации и выраженный с помощью последовательности условных физических символов (алфавита), образующих некоторую упорядоченную совокупность»

Информация в форме сообщения обладает рядом свойств, к числу которых следует отнести:

– ***материальность*** - способность воздействовать на органы чувств;

– ***доступность*** – если она содержится на информационном носителе;

– ***ценность*** – определяется степенью ее полезности для владельца;

– ***измеримость*** - возможность количественной оценки параметров сообщения (количество знаков, составляющих сообщение);

– ***сложность*** - наличие набора знаков и алгоритмов их кодирования и декодирования;

– ***проблемная ориентированность*** - содержание сведений, относящихся к одной их задач человеческой деятельности.

B большинстве случаев со временем ценность информации уменьшается. Зависимость ценности информации от времени приближенно определяется выражением.



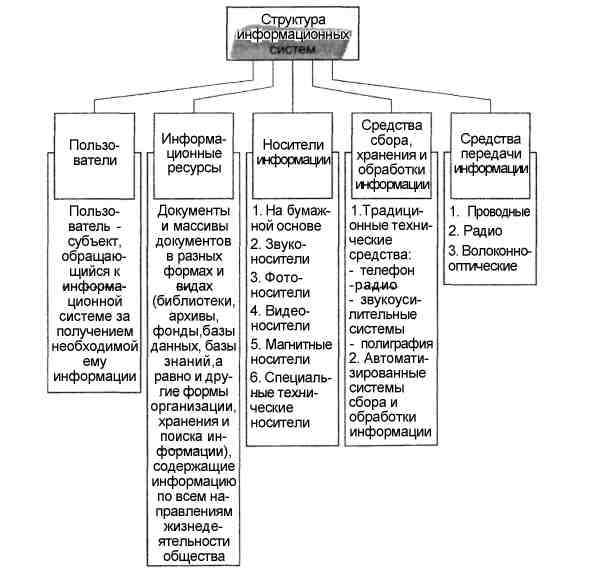
где C0 — ценность информации в момент ее возникновения (получения);

t — время от момента возникновения информации до момента определения ее стоимости;

τ — время от момента возникновения информации до момента ее устаревания.



**Информационная система** - это организационно упорядоченная совокупность информационных ресурсов, технических средств, технологий, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователей.



**Защищаемые помещения (ЗП) –** помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.)

**Основные технические средства и системы** **(ОТСС)**- технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной (секретной) информации

К ОТСС могут относиться

средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных),

технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической видео-, смысловой и буквенно-цифровой информации) используемые для обработки конфиденциальной (секретной) информации.

**Вспомогательные технические средства и системы** **(ВТСС)** - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в выделенных помещениях.

К ним относятся:

различного рода телефонные средства и системы;

средства и системы передачи данных в системе радиосвязи;

средства и системы охранной и пожарной сигнализации;

средства и системы оповещения и сигнализации;

контрольно-измерительная аппаратура;

средства и системы кондиционирования;

средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.д.);

средства электронной оргтехники.

Технический контроль проводится относительно мест возможного размещения аппаратуры разведки:

• носимой - на границе контролируемой зоны;

• возимой - в местах возможного нахождения аппаратуры разведки (стоянки автомобилей, соседние здания или сооружения).

Контроль защищенности от случайного (непреднамеренного) прослушивания проводится относительно мест возможного пребывания лиц, не допущенных к конфиденциальной информации.

При оценке мероприятии по информационной защите помещений учитываются следующие **возможные технические каналы утечки** или нарушения целостности информации:

• **акустическое** излучение речевого сигнала по воздушной среде;

• **электрические** сигналы, возникающие в результате преобразования акустических сигналов в электрические устройствами, обладающими микрофонным эффектом, и распространяющиеся по проводным линиям, выходящим за пределы контролируемой зоны:

• **вибрационные** сигналы, возникающие посредством преобразования акустических сигналов в колебания упругих сред ограждающих конструкций выделенных помещений;

• **электромагнитные** излучения случайных источников (паразитных генераторов). модулированные звуковым сигналом.

Для указанных технических каналов утечки информации существуют различные виды сред распространения сигналов таких как:

• **проводные сети**: электрические силовые, низковольтные (телефонные. охранные, пожарные, радиотрансляция, часофикация). сети ЭВМ (витая пара, коаксиальный, волоконно-оптические), кабели спецсвязи:

• **инженерные коммуникации**: отопление, водопровод, канализация, короба и трубы кабельных коммуникаций, специальные проемы и отверстия в стенах и перекрытиях, воздуховоды приточные и вытяжные:

• **элементы конструкции зданий**: стены капитальные, перегородки, окна (рамы, стекла), двери и перегородки, потолки;

• **воздушная среда**, по которой распространяются электромагнитные излучения технических средств (модуляция случайных генераторов, акустоэлектрические преобразования, побочные электромагнитные излучения, переизлучения под воздействием внешних источников).

# Классификация технических каналов утечки информации.

Информация передается полем или веществом. Это может быть либо акустическая волна, либо электромагнитное излучение, либо лист бумаги с текстом и т.п. Другими словами, используя те или иные физические поля, человек создает систему передачи информации или систему связи. Система связи в общем случае состоит из передатчика, канала передачи информации, приемника и получателя информации. Легитимная система связи создается и эксплуатируется для правомерного обмена информацией. Однако ввиду физической природы передачи информации при выполнении определенных условий возможно возникновение системы связи, которая передает информацию вне зависимости от желания отправителя или получателя информации – **технический канал утечки информации**.

**Утечка** - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

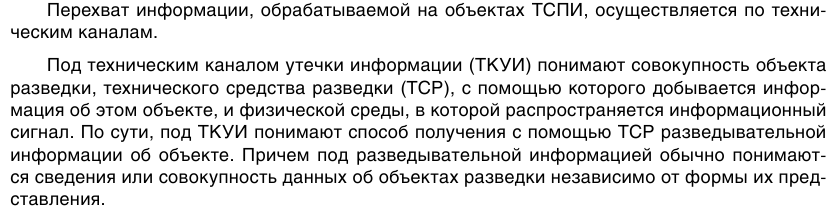


Рис. 1.Структура технического канала утечки информации.

Рис. 2.Классификация технических каналов утечки информации.

**Основные показатели технических каналов утечки информации**

Технический канал утечки информации характеризуется показателями,

которые позволяют оценить риск утечки. Такими показателями

являются:

– пропускная способность технического канала утечки;

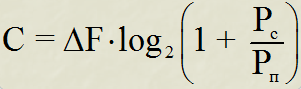
– длина технического канала утечки информации;

– относительная информативность технического канала утечки

информации.

***Предельная пропускная способность канала*** связи в битах в секунду

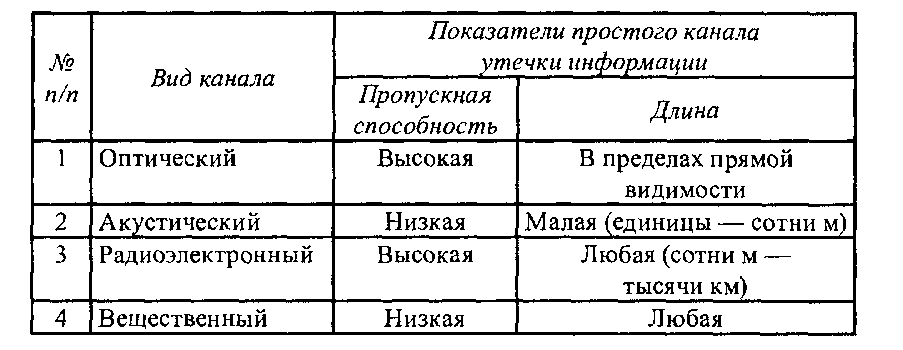
определяется по формуле:



где ***∆F***- ширина полосы пропускания канала связи в Гц;

Рс и Рп - мощности сигнала и помехи в полосе пропускания канала.

Таблица 1. Качественная оценка пропускной способности и длины технических каналов утечки информации



**Комплексное использование технических каналов утечки информации**

Комплексное использование параллельных каналов утечки информации основывается на следующих принципах:

* комплексируемые каналы дополняют друг друга по своим возможностям;
* эффективность комплексирования повышается при уменьшении зависимости между источниками информации и демаскирующими признаками в разных каналах.
* Комплексирование каналов утечки информации обеспечивает:
* увеличение вероятности обнаружения и распознавания объектов за счет расширения их текущих признаковых структур;
* повышение достоверности семантической информации и точности измерения признаков, в особенности в случае добывания информации из недостаточно надежных источников.

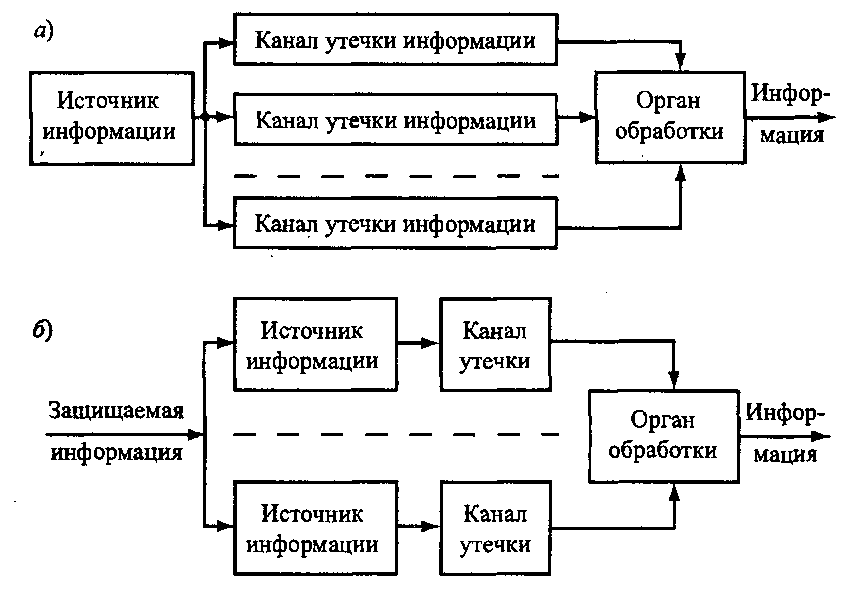


Рис. 3.Варианты комплексного использования каналов утечки информации.

При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

— акустическое излучение информативного речевого сигнала;

— электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы КЗ (контролируемая зона — это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств);

— виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

— несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

— воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;

— побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;

— наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

— радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;

— радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;

— радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

— прослушивание ведущихся телефонных и радиопереговоров;

— просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

— хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

Перехват информации или воздействие на нее с использованием технических средств могут вестись:

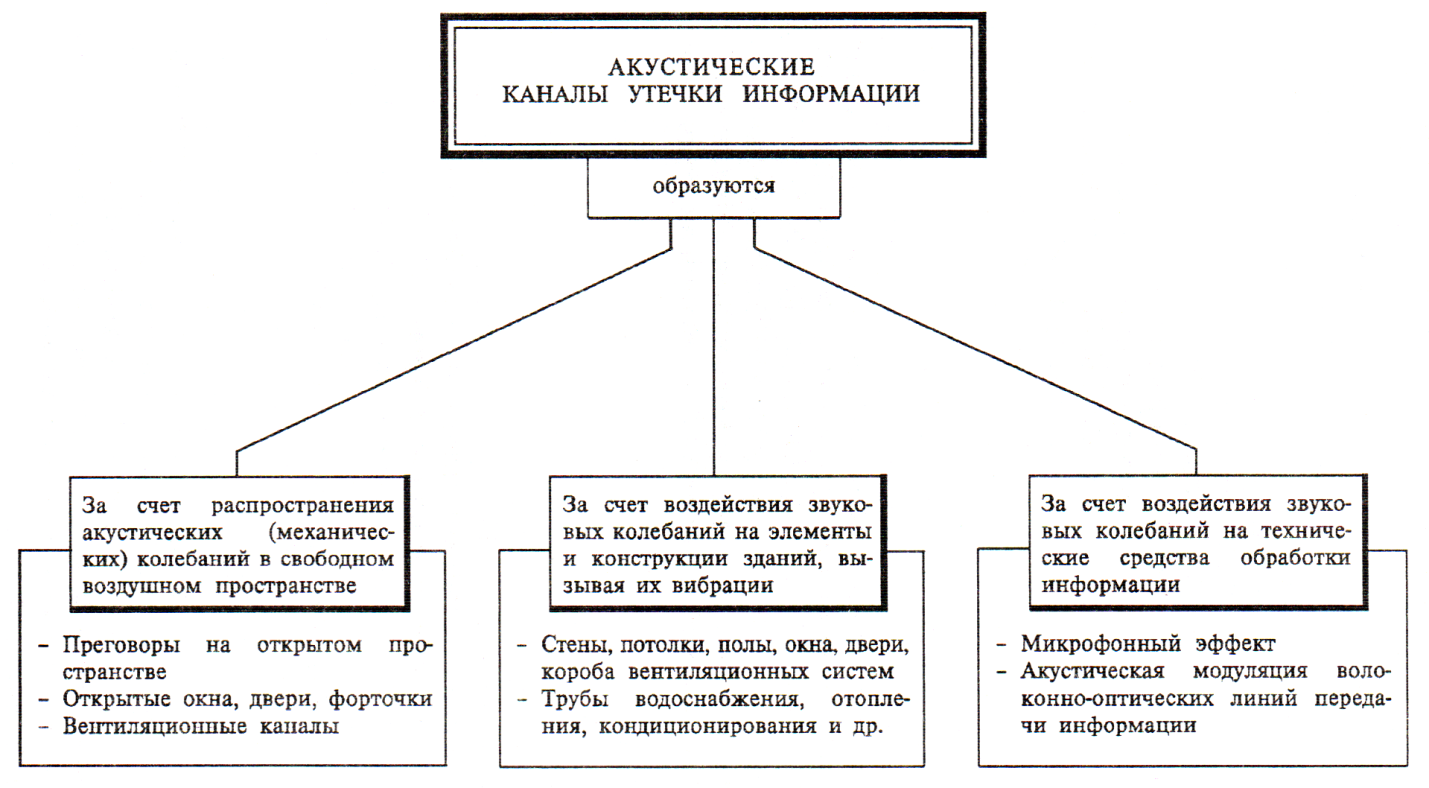
— из-за границы КЗ из близлежащих строений и транспортных средств;

— из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;

— при посещении учреждения (предприятия) посторонними лицами;

— за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

1. Акустические каналы утечки информации



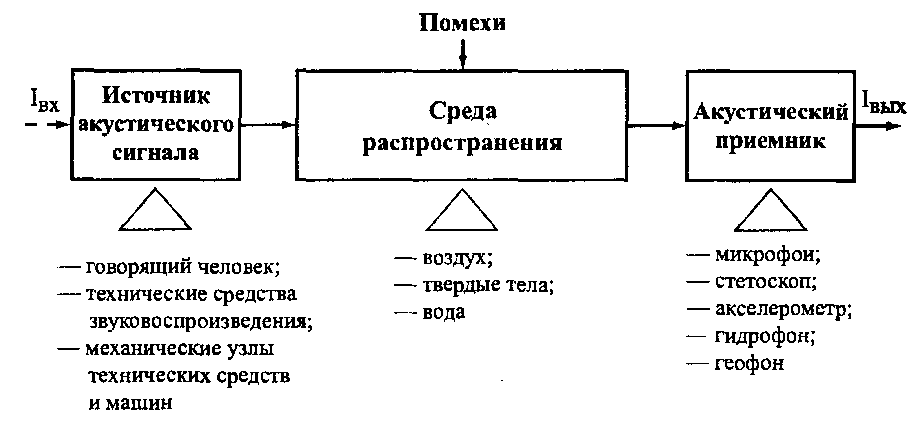


Рис.4*.* Структура акустического канала утечки информации

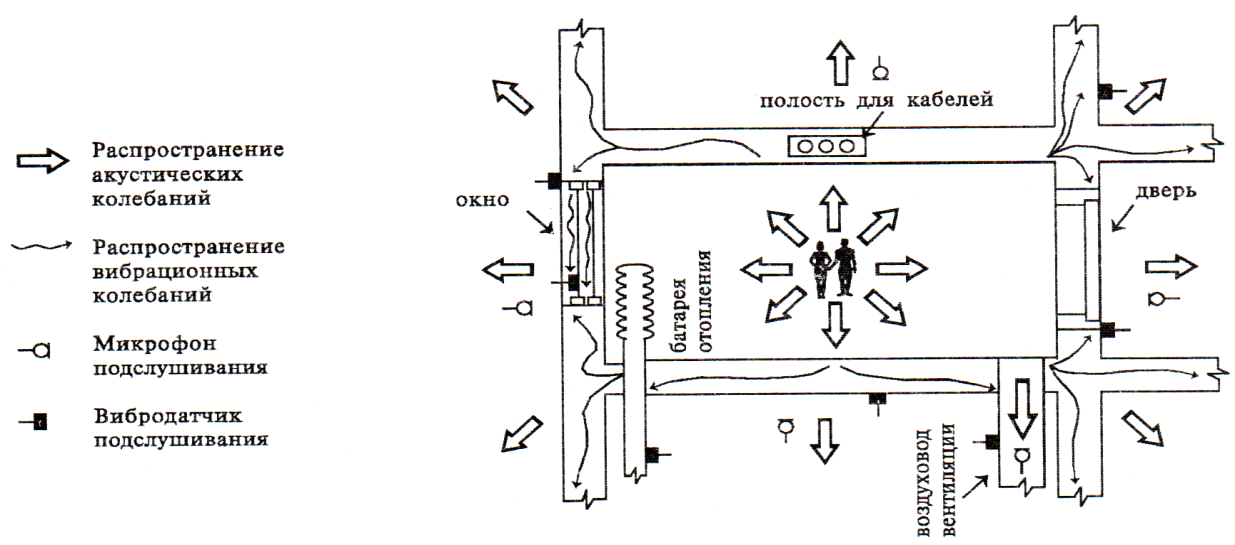


Рис. 6. Схема акустических и вибрационных каналов утечки информации

2. Оптические каналы утечки информации

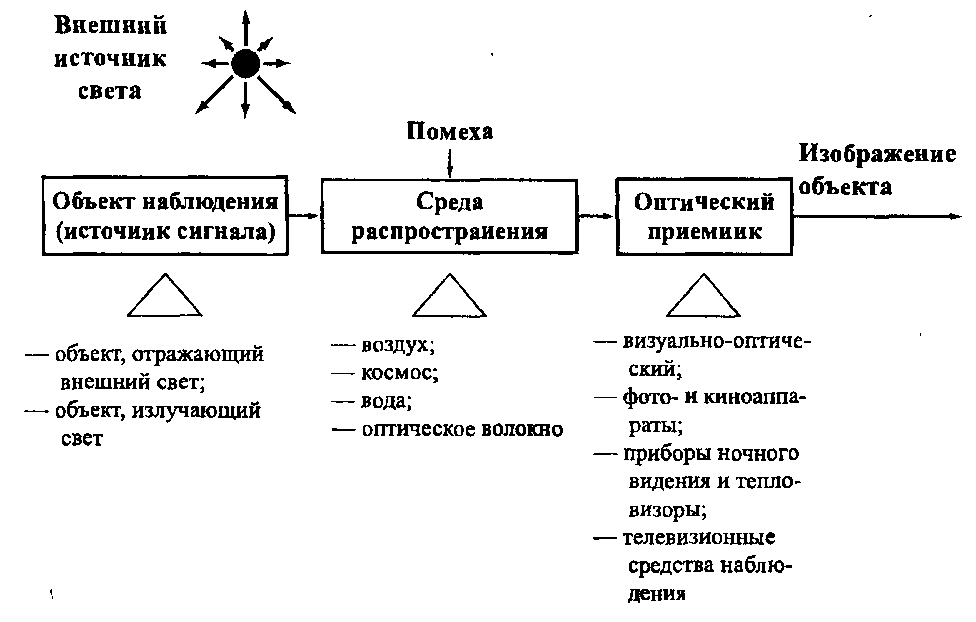


Рис. 2.Структура оптического канала утечки информации

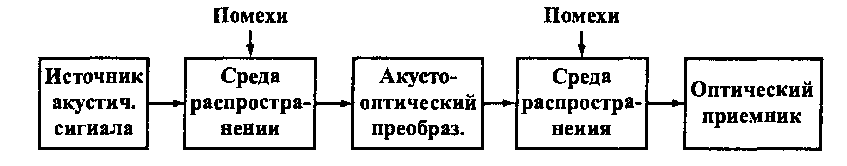


Рис. 3. Структурная схема приема акустической информации с использованием оптико - электронного канала.

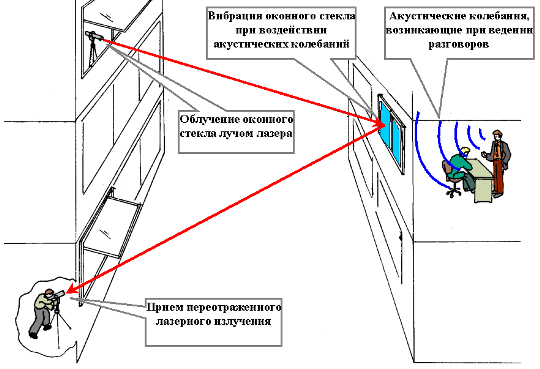


Рис. 4. Оптико-электронный канал утечки акустической информации

3. Радиоэлектронные каналы утечки информации.

В **радиоэлектронном канале** переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 100 – 10 км (частоты от 3 до 30 Гц) до миллиметровых с длиной волны 10 – 1 мм (частоты от 30 до 300 ГГц).

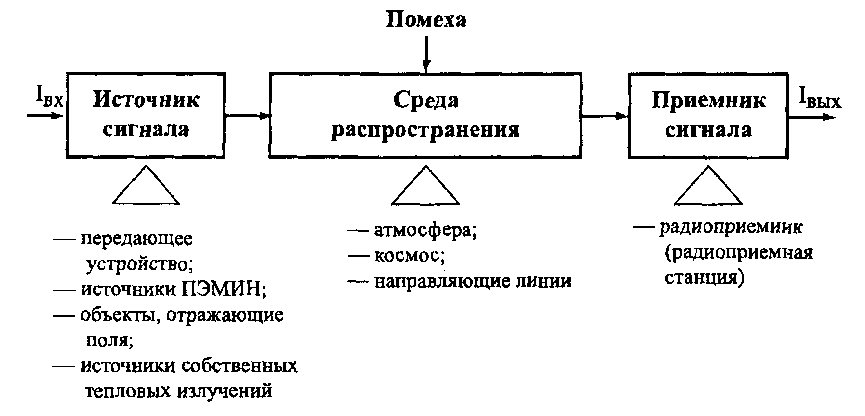


Рис. 15. Структура радиоэлектронного канала утечки информации.

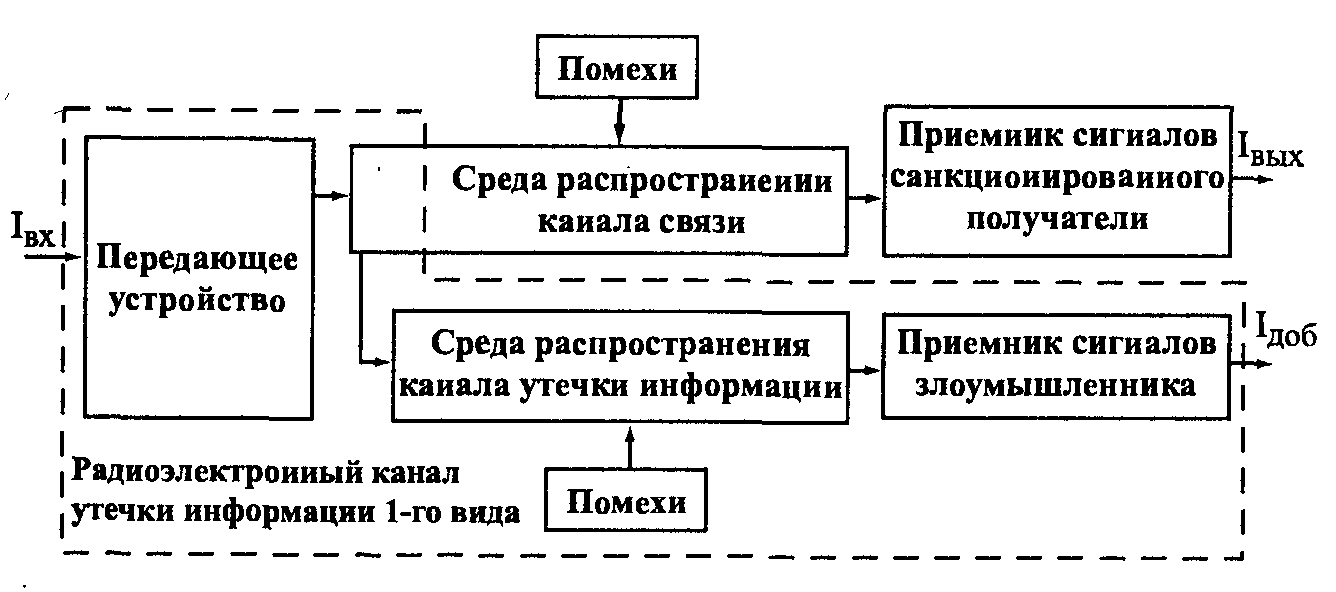


Рис. 16.Структура радиоэлектронного канала утечки информации 1-го вида.

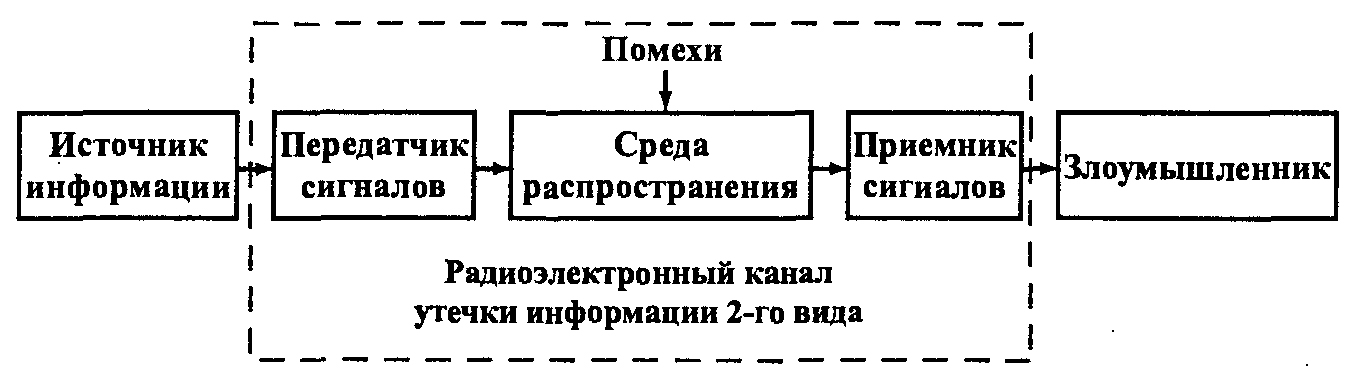


Рис. 16.Структура радиоэлектронного канала утечки информации 2-го вида.

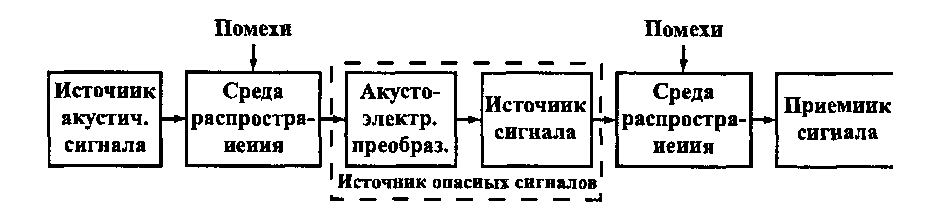
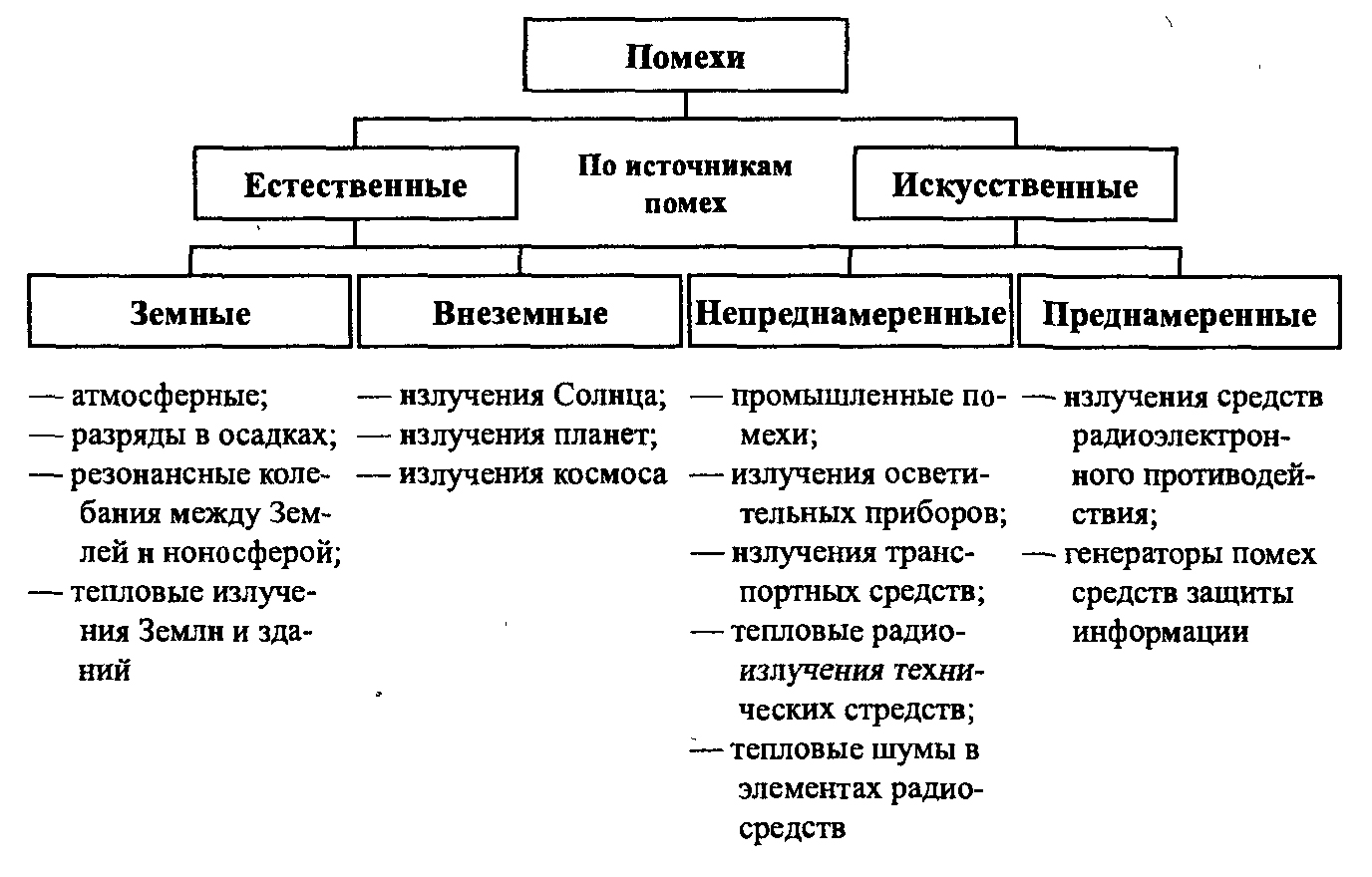


Рис. 18.Структура акусто-радиоэлектронного канала утечки информации.

Известны следующие **радиоэлектронные каналы** утечки информации:

* микрофонный эффект (составной акусто-радиоэлектронный канал)
* элементов электронных схем;
* электромагнитное излучение низкой и высокой частоты;
* возникновение паразитной генерации усилителей различного назначения;
* цепи питания и цепи заземления электронных схем;
* взаимное влияние проводов и линий связи;
* высокочастотное навязывание.

Рис. 23.Классификация помех по их источникам

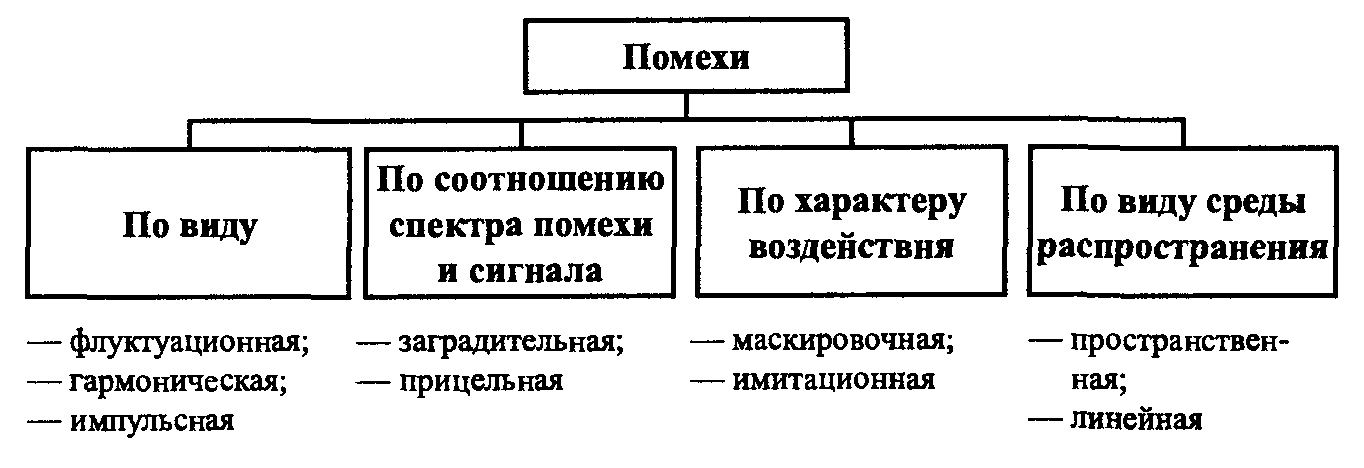


Рис. 24. Классификация помех по их параметрам.

4. Вещественные каналы утечки информации.

Основными источниками информации вещественного канала утечки информации являются следующие:

– черновики различных документов и макеты материалов, узлов, блоков,

устройств, разрабатываемых в ходе научно-исследовательских и опытно-

конструкторских работ, ведущихся в организации;

*–* отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, забракованные листы при

оформлении документов и их размножении;

– отходы промышленного производства опытного и серийного выпуска

продукции, содержащей защищаемую информацию в газообразном, жидком и твердом виде;

– содержащие защищаемую информацию дискеты и жесткие диски ПЭВМ,

нечитаемые из-за их физических дефектов и искажений загрузочных или других секторов;

– бракованная продукция и ее элементы;

– радиоактивные материалы.

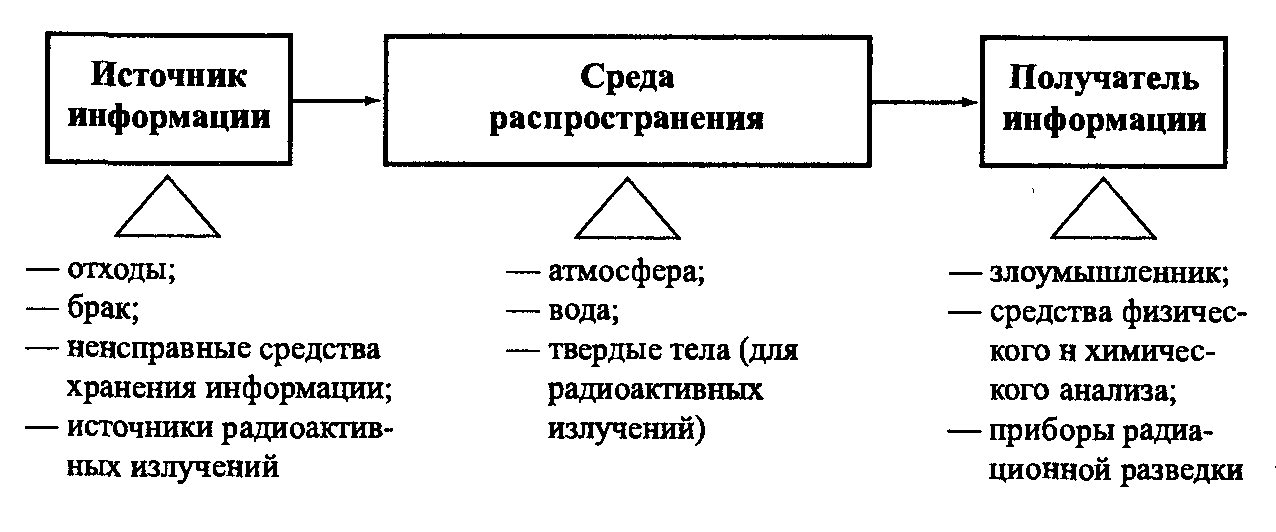


Рис. 25.Структура вещественного канала утечки информации

# 10. Иностранная техническая разведка

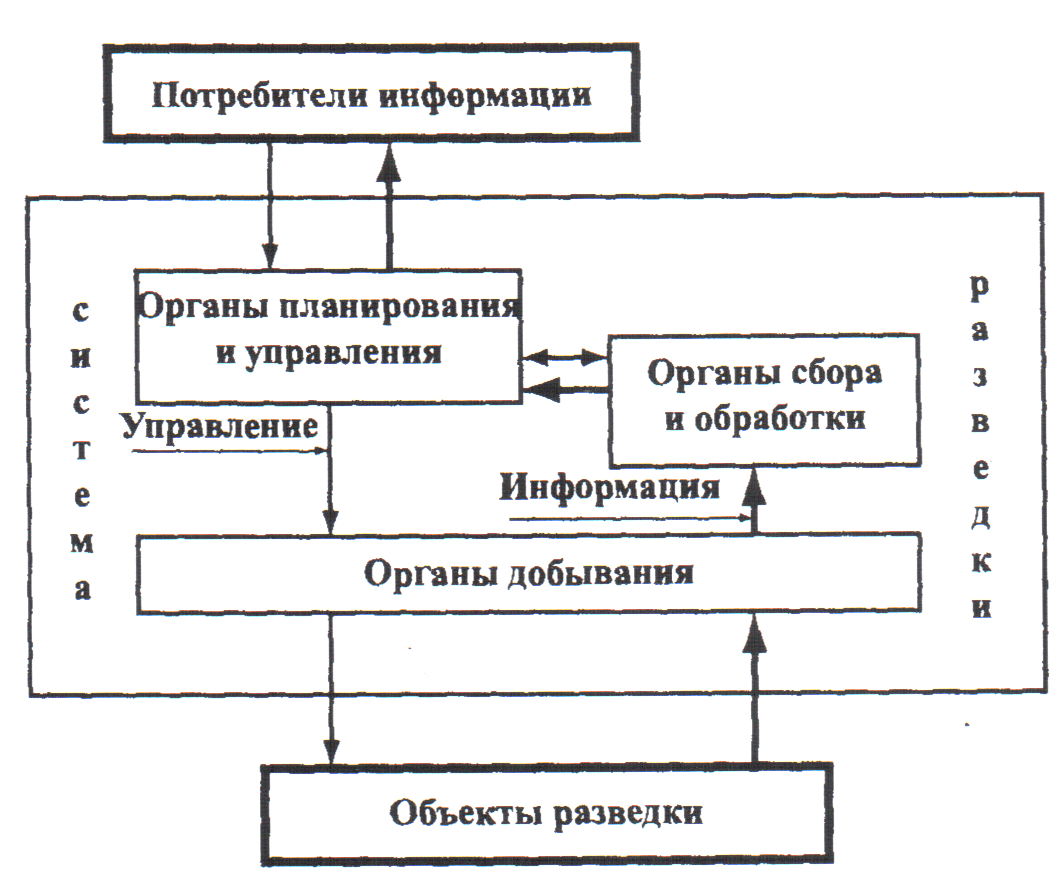
****

Рис. 5. Структура системы разведки

**Задачи разведки:**

* Добывание информации (политической, экономической, военной) для принятия стратегических, оперативных или тактических решений в соответствующих областях деятельности.
* Получение преимущества над противником на основе использования в своих целях его научно-технических, технологических и других достижений.

Для добывания информации разведка противника может использовать легальные, полулегальные и нелегальные методы.

**К легальным методам** относятся: изучение публикаций в средствах массовой информации (СМИ); участие в научно-технических конференциях; анализ общественно-политических, научных и технических изданий; посещение выставок; исследование сообщений электронных СМИ.

**К полулегальным методам** можно отнести: беседы с сотрудниками в неофициальной обстановке; мнимые переговоры о покупке продукции; ложные конкурсы; приглашение на работу ведущих специалистов; получение информации от общих поставщиков, потребителей.

**К нелегальным методам относятся**: хищение образцов продукции и (или) технологического оборудования; хищение документов, содержащих интересующую информацию; копирование документов, содержащих интересующую информацию; заброс агентов проникновения на объект противника; внедрение агентов в структуры противника; съем информации по техническим каналам; проникновение в автоматизированные системы.

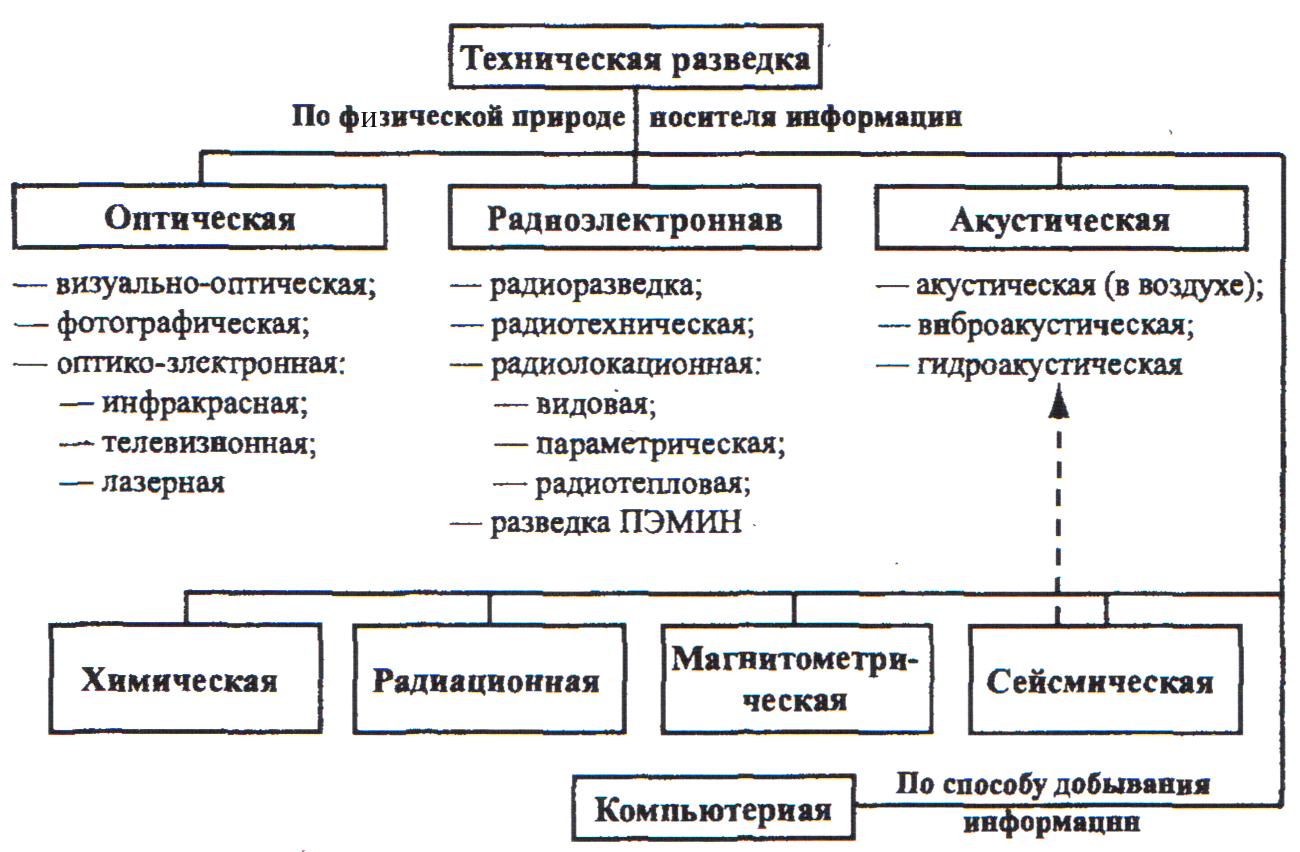
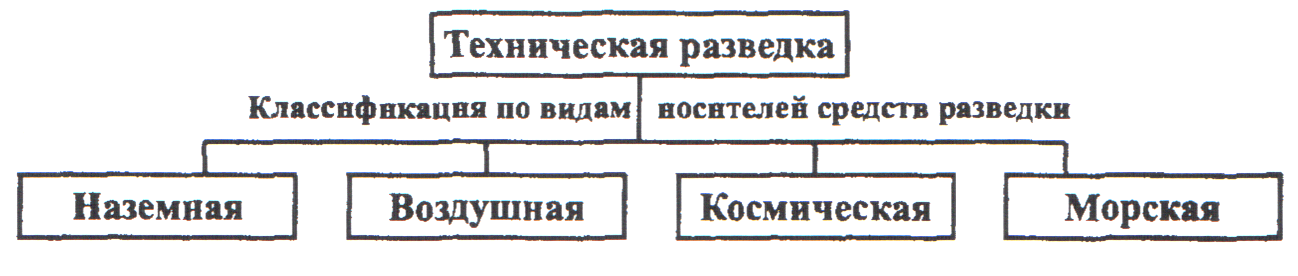


Рис. 6. Классификация технической разведки по носителям информации

Рис. 7. Классификация технической разведки по видам носителей средств разведки

***Технология добывания информации предусматривает следующие этапы:***

* организация добывания;
* добывание данных и сведений;
* информационная работа.

***Организация добывания*** информации включает:

* декомпозицию (структурирование) задач, поставленных пользователями информации;
* разработку замысла операции по добыванию информации;
* планирование;
* постановку задач исполнителям;
* нормативное и оперативное управление действиями исполнителей и режимами работы технических средств.

Технические средства существенно расширяют и дополняют возможности человека по добыванию информации, обеспечивая:

* съем информации с носителей, которые недоступны органам чувств человека;
* добывание информации без нарушения границ контролируемой зоны;
* передачу информации практически в реальном масштабе времени в любую точку земного шара;
* анализ и обработку информации в объеме и за время, недостижимых человеком;
* консервацию и сколь угодно долгое хранение добываемой информации.

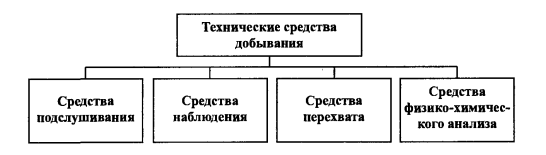


Рис. 8. Классификация средств добывания информации по назначению.

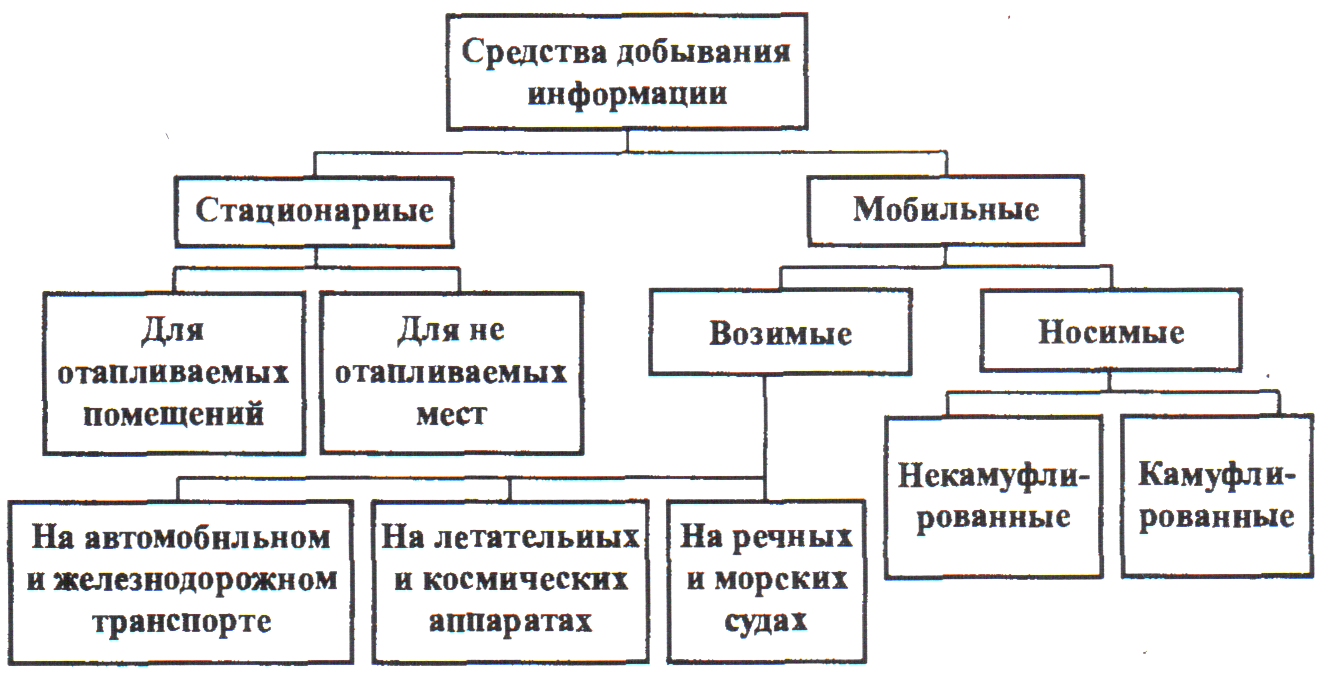


Рис. 9.Классификация средств добывания по условиям эксплуатации.

# Информационное противоборство стран.

Человечество с незапамятных времен сталкивалось с проблемой информационных войн на всех уровнях, и лук, стрелы, мечи, пушки и танки, в конце концов, только завершали физический разгром сообщества, уже потерпевшего поражение в информационной войне.

На концептуальном уровне можно сказать, что государства стремятся приобрести информации, обеспечивающую выполнение их целей, воспользоваться ей и защитить ее. Эти использование и защита могут осуществляться в экономической, политической и военной сферах.

Знание об информации, которой владеет противник, является средством, позволяющим усилить нашу мощь и понизить мощь врага или противостоять ей, а также защитить ценности, включая информацию.

Информационное оружие воздействует на информацию, которой владеет враг и его информационные функции. При этом наши информационные функции защищаются, что позволяет уменьшить его волю или возможности вести борьбу.

Поэтому дадим определение ***информационной войне*** - это любое действие по использованию, разрушению, искажению вражеской информации и ее функций; защите нашей информации против подобных действий; и использованию наших собственных военных информационных функций.

Это определение является основой для следующих утверждений.

* **Информационная война** - это комплексное совместное применение сил и средств информационной и вооруженной борьбы.
* **Информационная война** - это коммуникативная технология по воздействию на информацию и информационные системы противника с целью достижения информационного превосходства в интересах национальной стратегии, при одновременной защите собственной информации и своих информационных систем.
* **Информационная война** - только средство, а не конечная цель, аналогично тому как бомбардировка - средство, а не цель.
* **Информационную войну** можно использовать как средство для проведения стратегической атаки или противодействия.

Первым использовал термин "информационная война" американский эксперт Томас Рона в отчете, подготовленным им в 1976 году для компании Boeing, и названный "Системы оружия и информационная война". Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью, как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина "информационная война".

Публикация отчета Т. Рона послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься "секретными материалами". Военно-воздушные силы США начали активно обсуждать этот предмет уже с 1980 года.

С военной точки зрения термин "информационная война" в наше время был употреблен в середине 80-х годов XX в. в связи с новыми задачами Вооруженных сил США после окончания "холодной" войны. Это явилось результатом работы группы американских военных теоретиков в составе Г.Е. Экклз, Г.Г. Саммерз и др. В дальнейшем термин начал активно употребляться после проведения операции "Буря в пустыне" в 1991 г. в Ираке, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года.

Спустя несколько лет, в феврале 1996 года, Министерство обороны США ввело в действие "Доктрину борьбы с системами контроля и управления". Публикация определяет борьбу с системами контроля и управления как "объединенное использование приемов и методов безопасности, военного обмана, психологических операций, радиоэлектронной борьбы и физического разрушения объектов системы управления, поддержанных разведкой, для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению над полем боя, при одновременной защите своих сил и сил союзников, а также препятствование противнику делать тоже самое" [3].

Наиболее важным является то, что эта публикация определила понятие войны с системами контроля и управления. И это было впервые, когда Министерство обороны США определило возможности и доктрину ИВ.

В конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции "Force XXI"). В ее основу было положено разделение всего театра военных действий на две составляющих - традиционное пространство и киберпространство, причем последнее имеет даже более важное значение. Р. Банкер предложил доктрину "киберманевра", которая должна явиться естественным дополнением традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

Таким образом, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включается и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин "human network").

В октябре 1998 года, Министерство обороны США вводит в действие "Объединенную доктрину информационных операций". Первоначально эта публикация называлась "Объединенная доктрина информационной войны". Позже она была переименована в "Объединенную доктрину информационных операций". Причина изменения состояла в том, чтобы разъяснить отношения понятий информационных операций и информационной войны.

Они были определены, следующим образом:

***информационная операция:*** действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем;

В более современной интерпретации ***информационная операция*** (англ. Information Operations (Info Ops)) понимается как интегрированное использование возможностей электронного оружия, компьютерных сетевых операций (CNO), психологических операций (PSYOP, МИСО), операций с военной дезинформации и дезорганизации та операции безопасности (OPSEC) для использования возможностей влияния на человеческое сознание с целью разрушения, разложения, или вообще перехват влияния на принятие решений противника, при этом защищая свое собственное (решение).



***информационная война:*** комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

Сейчас существует довольно много разных определений ИВ и с технико-технологической точки зрения. В коридорах Пентагона ходит, например, такое шутливое определение **"Информационная война - это компьютерная безопасность плюс деньги"**.

А если серьезно, то военные подходят к ИВ так, как это было сформулировано еще в Меморандуме N30 (1993 г) заместителей Министра Обороны и Комитета начальников штабов Вооруженных Сил США .

Под информационной войной здесь понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственной информации и информационных систем.

В гуманитарном смысле "информационная война" понимается как те или иные активные методы трансформации информационного пространства. В информационных войнах этого типа речь идет об определенной системе (концепции) навязывания модели мира, которая призвана обеспечить желаемые типы поведения, об атаках на структуры порождения информации, процессы рассуждений.

Основными формами ведения технической ИВ являются радиоэлектронная борьба, война с использованием средств электронной разведки и наведения, нанесения удаленных точечных ударов с воздуха, психотропная война, борьба с хакерами, кибернетическая война.

Прежде чем всерьез анализировать различные определения информационной войны с технической точки зрения отметим присущее ей важное свойство:

ведение информационной войны никогда не бывает случайным или обособленным, а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле боя, либо в экономической, политической, социальной сферах.

Поэтому в качестве основного и наиболее общего определения ИВ предложу следующее:

"**Информационная война** - это всеобъемлющая целостная стратегия, обусловленная все возрастающей значимостью и ценностью информации в вопросах командования, управления и политики".

Поле действия информационных войн при таком определении оказывается достаточно широким и охватывает следующие области:

1) инфраструктуру систем жизнеобеспечения государства - телекоммуникации, транспортные сети, электростанции, банковские системы и т.д.;

2) промышленный шпионаж - хищение патентованной информации, искажение или уничтожение особо важных данных, услуг; сбор информации разведывательного характера о конкурентах и т.п.;

3) взлом и использование личных паролей VIР-персон, идентификационных номеров, банковских счетов, данных конфиденциального плана, производство дезинформации;

4) электронное вмешательство в процессы командования и управления военными объектами и системами, "штабная война", вывод из строя сетей военных коммуникаций;

5) всемирная компьютерная сеть Интернет, в которой, по некоторым оценкам, действуют 150.000 военных компьютеров, и 95% военных линий связи проходят по открытым телефонным линиям.

Какой бы смысл в понятие "информационная война" ни вкладывался, оно родилось в среде военных и обозначает, прежде всего, жесткую, решительную и опасную деятельность, сопоставимую с реальными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психотронная война, информационно-психологическая война, кибернетическая война и т.

Итак, **информационная война** - это такая форма конфликта, в которой происходят прямые атаки на информационные системы для воздействия на знания или предположения противника.

Информационная война может проводиться как часть большего и более полного набора военных действий.

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом киберпространстве, чтобы вести "бесконтактную" войну, в которой количество жертв (в прямом значении слова) сведено до минимума. "Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий, - сказал один из руководителей Пентагона. - Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума".

Современные средства выполнения информационных функций сделали информацию уязвимой к прямому доступу и манипуляции с ней. Современные технологии позволяют противнику изменить или создать информацию без предварительного получения фактов и их интерпретации.

Вот краткий список характеристик современных информационных систем, приводящим к появлению подобной уязвимости:

* концентрированное хранение информации;
* скорость доступа;
* повсеместная передача информации;
* большие возможности информационных систем выполнять свои функции автономно.

***Существуют три цели информационной войны:***

* контролировать информационное пространство, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий (контринформация).
* использовать контроль за информацией для ведения информационных атак на врага
* повысить общую эффективность вооруженных сил с помощью повсеместного использования военных информационных функций.

***Задача:*** *Предположим, что мы хотим ограничить стратегические возможности врага по переброске войск путем уменьшения запасов топлива.*

**Алгоритм стратегической атаки:** Сначала мы должны выявить нефтеперегонные заводы, которые будут наиболее подходящими целями при этой атаке. Потом нужно установить, какие заводы производят больше всего топлива. Для каждого завода нам надо выявить местоположение перегонных емкостей. Мы организуем атаку и, при значительной экономии сил, выводим заводы из строя, взрывая их только перегонные емкости, и оставляя все остальное оборудование нетронутым. Это классический пример стратегической атаки.

**Алгоритм информационной атаки** Все современные нефтеперегонные заводы имеют большие автоматизированные системы управления. Эти информационные функции являются потенциальной целью в информационной войне. На ранней стадии конфликта мы выполнили разведывательную информационную операцию по проникновению и анализу системы управления нефтеперегонным заводом. В ходе анализа мы обнаружили несколько уязвимых информационных зависимостей, дающих нам средства воздействия на работу нефтеперегонного завода в нужное нам время. Позднее, в ходе конфликта, в ходе одной из операций по блокированию вражеской группировки мы использовали одно из уязвимых мест. Мы просто остановили эти заводы. Это, тоже классический пример стратегической атаки.

***Задача:*** *заставить врага думать, что авиаполк находится там, где он совсем не находится, и действовать на основании этой информации таким образом, чтобы это было выгодно нам.*

***Косвенная информационная атака***: используя инженерные средства, мы можем построить макеты самолетов и ложные аэродромные сооружения, и противник будет наблюдать ложный аэродром и считать его настоящим. Только тогда эта информация станет той, которую должен иметь противник по нашему мнению.

***Прямая информационная атака***: если мы создаем информацию о ложном авиаполке в хранилище информации у противника, то результат будет точно такой же. Но средства, задействованные для получения этого результата, будут отличаться.

Другим примером прямой информационной атаки может быть изменение информации во вражеской базе данных об имеющихся коммуникациях в ходе боевых действий (внесение ложной информации о том, что мосты разрушены) для изоляции отдельных вражеских частей. Этого же можно добиться бомбардировкой мостов. И в том, и в другом случае вражеские аналитики, принимая решение на основе имеющейся у них информации, примут одно и то же решение - производить переброску войск через другие коммуникации.

Следует отличать **информационную войну** от **компьютерной преступности**.

Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть составной частью обширного плана атаки. Напротив, ведение информационной войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле брани, либо в экономической, политической или социальной сферах.

Театр информационных боевых действий простирается от секретного кабинета до домашнего персонального компьютера и ведется на различных фронтах.

Электронное поле боя представлено постоянно растущим арсеналом электронных вооружений, преимущественно засекреченных. Говоря военным языком, они предназначены для боевых действий в области командования и управления войсками, или "штабной войны". Последние конфликты уже продемонстрировали всю мощь и поражающую силу информационных боевых действий - война в Персидском заливе и вторжение на Гаити. Во время войны в Персидском заливе силы союзников на информационном фронте провели комплекс операций в диапазоне от старомодной тактики разбрасывания пропагандистских листовок до вывода из строя сети военных коммуникаций Ирака с помощью компьютерного вируса.

**Атаки инфраструктуры наносят удары по жизненно важным элементам**, таким как телекоммуникации или транспортные системы. Подобные действия могут быть предприняты геополитическими или экономическими противниками или террористическими группами. Примером служит вывод из строя междугородной телефонной станции компании AT&T в 1990 году. В наши дни любой банк, любая электростанция, любая транспортная сеть и любая телевизионная студия представляют собой потенциальную мишень для воздействия из киберпространства.

**Промышленный шпионаж** и другие виды разведки грозят великим множеством тайных операций, осуществляемых корпорациями или государствами в отношении других корпораций или государств; например, сбор информации разведывательного характера о конкурентах, хищение патентованной информации и даже акты саботажа в форме искажения или уничтожения данных. Иллюстрацией этой угрозы служит документально доказанная деятельность французских и японских агентов на протяжении восьмидесятых годов.

Сбор разведывательной информации также выходит на новые рубежи. Лаборатория Линкольна в Массачусетском технологическом институте разрабатывает аппарат для воздушной разведки размером с пачку сигарет. Другая лаборатория работает над химическими веществами, которые можно ввести в провизию неприятельских войск, чтобы позволить датчикам отслеживать их перемещение по дыханию или выделению пота. Помимо этого уже имеются спутниковые системы слежения, имеющие разрешающую способность в несколько сантиметров.

**Конфиденциальность все более уязвима** по мере появления возможности доступа к постоянно растущим объемам информации в постоянно растущем числе абонентских пунктов. Важные персоны, таким образом могут стать объектом шантажа или злобной клеветы, и никто не гарантирован от подложного использования личных идентификационных номеров.

Как бы то ни было, термин "информационная война" обязан своим происхождением военным и обозначает жестокую и опасную деятельность, связанную с реальными, кровопролитными и разрушительными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психологические операции и так далее.

К составным частям информационной войны относятся:

1) ***психологические операции*** - использование информации для воздействия на аргументацию солдат врага.

2) ***электронная война*** - не позволяет врагу получить точную информацию

3) ***дезинформация*** - предоставляет врагу ложную информацию о наших силах и намерениях

4) ***физическое разрушение*** - может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем.

5) ***меры безопасности*** - стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях.

6***) прямые информационные атаки*** - прямое искажение информации без видимого изменения сущности, в которой она находится.

Как ранее говорилось, существует два способа повлиять на информационные функции врага - косвенно или напрямую. Проиллюстрируем разницу между ними на примере.

***Информационным оружием*** называются средства:

– уничтожения, искажения или хищения информационных массивов;

– преодоления систем защиты;

– ограничения допуска законных пользователей;

– дезорганизации работы технических средств, компьютерных систем.

***Атакующим информационным оружием*** можно назвать:

– компьютерные вирусы, способные размножаться, внедряться  
программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.д.;

– логические бомбы – программные закладные устройства,  
которые заранее внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

– средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;

– средства нейтрализации тестовых программ;

– различного рода ошибки, сознательно вводимые противником в программное обеспечение объекта.

Информационное оружие от обычных средств поражения отличает:

**скрытность** - возможность достигать цели без видимой подготовки и объявления войны;

**масштабность** - возможность наносить невосполнимый ущерб, не признавая национальных границ и суверенитета, без ограничения пространства во всех сферах жизнедеятельности человека;

**универсальность** - возможность многовариантного использования как военных, так и гражданских структур страны нападения против военных и гражданских объектов страны поражения;

**низкая стоимость создания и высокая эффективность применения.**

**доступность** - лёгкое распространение и высокий уровень контроля над процессом исполнения.

**длительность -** возможность долгосрочного применения информационного оружия без утери эффективности его применения.

**возможность использования в мирное время и внезапность применения в случае военных действий**

Выделяют четыре основных вида информационного оружия:

***1. Воздействие на человеческую психику:***

К данному типу информационного оружия относятся методы, способы и средства воздействия на психическое состояние человека с целью изменения или подрыва этого состояния:

- все виды средств массовой информации;

- печатный материал, к которому относятся листовки, плакаты, афиши, раздаточный материал и т.д.;

- средства связи;

- музыка, кинофильмы, реклама и т.д;

- компьютерные игры.

***2. Дезинформирование систем принятия решений:***

К данному типу относятся методы воздействия на групповые и индивидуальные системы принятия решений, с целью выбора решения, выгодного дезинформатору:

- навязывание информации;

- искажение информации;

- блокирование информации;

- утаение информации;

- подмена информации.

К основным средствам ведения противоборства оружием такого типа относятся средства массовой информации, телекоммуникационные системы, средства связи.

***3. Радиоэлектронная борьба:***

- радиоэлектронная разведка (включает в себя перехват и анализ информации, поступающей через телекоммуникационные системы, дезинформирование);

- радиоэлектронное противодействие (создание помех при передаче информации);

- подавление элементов телекоммуникационных систем, радиовещания, телевизионных сигналов, линий связи и т.д. (использование заглушек).

***4. Воздействие на программно-техническое оснащение телекоммуникационных систем (далее – ТКС) и автоматизированных информационных систем (далее – АИС):***

Этот тип информационного оружия включает в себя средства и методы несанкционированного доступа к ТКС и АИС:

- хищение, искажение или уничтожение информации;

- ограничение или запрет доступа к компьютерным системам;

- дезориентация работы компьютерных систем;

- блокирование или вывод из строя компьютерных систем.

При этом по своей результативности информационное оружие сопоставимо с оружием массового поражения. *Доказано, что наибольшие потери вооруженные силы несут от воздействия поражающих элементов информационного оружия, действующих на системы управления и психику человека.*

Если рассматривать информационное оружие как совокупность средств, применяемых для нарушения (копирования, искажения или уничтожения) информационных ресурсов на стадиях их создания, обработки, распространения и (или) хранения, то в структуре инфосферы в качестве основных объектов воздействия при информационном противоборстве выступают:

* сети связи и информационно-вычислительные сети, используемые государственными организациями при выполнении своих управленческих функций;
* военная информационная инфраструктура, решающая задачи управления войсками;
* информационные и управленческие структуры банков, транспортных и промышленных предприятий;
* средства массовой информации и, в первую очередь, электронные.

***Активное информационное оружие*** – это единая система комплексного, комбинированного, пучкового, целевого и ударного применения всех сил и средств технического, коммуникативного, информационно – психологического воздействия на подсознание субъекта атаки. Это оружие разрушает интеллект, военную информационную инфраструктуру, решающую задачи управления войсками, одновременно поражает информационные правительственные коммуникации и гражданские системы противника.

Способ реализации активного информационного оружия можно разделить на три группы: математическое алгоритмическое, программное и аппаратное. Наиболее эффективно оружие применяется в комплексе, так как оно может нести в себе все групповые признаки. По целям использования оружие можно разделить на: атакующее, обороняющее и обеспечивающее.

Обеспечивающее оружие применяется против средств защиты информации атакуемой системы. В его состав входят средства преодоления системы защиты.

Активное информационное оружие применяется для нападения на информационные системы и подсистемы террористических организаций и вероятного противника.

Объектами поражения активным информационным оружием могут выступать:

* военное руководство вероятного противника;
* политическое руководство вероятного противника;
* лидеры террористических организаций;
* мировое общественное мнение при проведении специальных информационно-психологических операций.

***Информационное противодействие*** представляет собой специальные комплексные контрмероприятия, направленные на упреждение, профилактику, опережение и защиту от деструктивных замыслов противника на разум человека, принимающего управленческие решения.

Доминирующей целью операций по информационному противодействию является обеспечение безопасности собственных информационных ресурсов. Цель достигается за счет физической защиты объектов, скрытого наружного наблюдения, технической оснащенности, оперативной маскировки, дезинформации в сочетании с оперативными комбинациями, контрпропагандой в комплексе с радиоэлектронной борьбой.

Одним из наиболее эффективных и новейших средств ведения информационного противоборства является электромагнитное оружие, предназначенное для воздействия на информационные системы. Массовое применение этого оружия может нарушить функционирование информационно-процессорной инфраструктуры, парализовать военные системы управления и жизненно важные производства противника, что значительно снизит его боеготовность и эффективность проведения боевых операций.

Любая информационная система может быть атакована с помощью беспроводных технических средств силового деструктивного воздействия. Воздействие может осуществляться с помощью электромагнитных импульсов на такие элементы системы, как беспроводные и проводные линии связи, системы электропитания и заземления, непосредственно на электронные элементы различных блоков.

Силовое деструктивное воздействие в настоящее время является серьезным оружием против систем защиты информационных объектов. Такое оружие оправдывает свое название электромагнитной бомбы и по эффективности является более грозным для компьютерных сетей, чем программное разрушающее воздействие. В наибольшей степени это относится к мощным мобильным техническим средствам, которые могут действовать с неохраняемой территории и на значительном расстоянии.

***Информационно-психологическое воздействие*** представляет собой целенаправленную психологическую атаку на конкретные сферы психики человека, группы лиц или общественное сознание в целом. Воздействие может осуществляться по средствам информационных раздражителей с использованием всего спектра методов и форм технического, визуального, звукового, медикаментозного, физического, болевого, виртуального подавления воли.

**Последствия информационной войны**

Взрыв нескольких гранат нельзя назвать войной, кто бы их не бросал. Взрыв нескольких водородных бомб - это уже и начатая и завершенная война.

Информационную пропаганду 50-ых, 60-ых годов, которой занимались СССР и США, можно сравнить именно с несколькими гранатами. Поэтому никто не называет прошлое противостояние информационной войной, в лучшем случае оно заслуживает термина "холодная война".

День сегодняшний, с его телекоммуникационными вычислительными системами, психотехнологиями кардинально изменил окружающее пространство. Отдельные информационные ручейки превратились в сплошной поток. Если ранее было возможно "запрудить" конкретные информационные каналы, то сегодня все окружающее пространство информационно коллапсировалось. Время на информационное взаимодействие между самыми отдаленными точками приблизилось к нулю. В результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность - защиту от информации.

Почему надо защищать информационную систему от информации? Потому что любая поступающая на вход системы информация неизбежно изменяет систему. Целенаправленное же, умышленное информационное воздействие может привести систему к необратимым изменениям и к самоуничтожению.

Поэтому информационная война - это не что иное, как явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Исходя из приведенного определения информационной войны, применение информационного оружия означает подачу на вход информационной самообучающейся системы такой последовательности входных данных, которая активизирует в системе определенные алгоритмы, а в случае их отсутствия - алгоритмы генерации алгоритмов.

Оборонительной стороной информационной войны являются меры безопасности, имеющие своей целью защитить информацию - не позволить противнику провести успешную информационную атаку на наши информационные функции. Современные меры защиты, такие как операционная безопасность и коммуникационная безопасность - типичные средства по предотвращению и обнаружению косвенных действий врага, направленных на наши военные информационные функции. Напротив, такие меры защиты, как компьютерная безопасность включают в себя действия по предотвращению, обнаружению прямых информационных действий врага и организации контрдействий.

Создание универсального защитного алгоритма, позволяющего выявить системе-жертве факт начала информационной войны, является алгоритмически неразрешимой проблемой. К таким же неразрешимым проблемам относится выявление факта завершения информационной войны. Однако, несмотря на неразрешимость проблем начала и окончания информационной войны, факт поражения в ней характеризуется рядом признаков, присущих поражению в обычной войне. К ним относятся:

1) включение части структуры пораженной системы в структуру системы победителя (эмиграция из побежденной страны и в первую очередь вывоз наиболее ценного человеческого материала, наукоемкого производства, полезных ископаемых);

2) полное разрушение той части структуры, которая отвечает за безопасность системы от внешних угроз (разрушение армии побежденной страны);

3) полное разрушение той части структуры, которая ответственна за восстановление элементов и структур подсистемы безопасности /разрушение производства, в первую очередь, наукоемкого производства, а также научных центров и всей системы образования; прекращение и запрещение разработок и производств наиболее перспективных видов вооружения);

4) разрушение и уничтожение той части структуры, которая не может быть использована победителем в собственных целях;

5) сокращение функциональных возможностей побежденной системы за счет сокращения ее информационной емкости (в случае страны: отделение части территории, уничтожение части населения).

Обобщив перечисленные признаки, можно ввести понятие "степень поражения информационным оружием", оценив ее через информационную емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Информационное оружие даст максимальный эффект только тогда, когда оно применяется по наиболее уязвимым от него частям ИСС. Наибольшей информационной уязвимостью обладают те подсистемы, которые наиболее чувствительны к входной информации - это системы принятия решения, управления. На основании сказанного можно ввести понятие информационной мишени. Информационная мишень - множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Исходя из определения информационной мишени, намечаются основные направления работ, как по обеспечению се безопасности, так и по повышению ее уязвимости. Например, для того, чтобы повысить уязвимость противника, следует максимально расширить его информационную мишень, т.е. подтолкнуть его на включение в мишень как можно больше равноправных элементов, причем желательно открыть доступ в сферу управления таким элементам, которые легко поддаются перепрограммированию и внешнему управлению.

Заставить противника изменить свое поведения можно с помощью явных и скрытых, внешних и внутренних информационных угроз.

Причины внешних угроз в случае целенаправленного информационного воздействия (в случае информационной войны) скрыты в борьбе конкурирующих информационных систем за общие ресурсы обеспечивающие системе допустимый режим существования.

Причины внутренних угроз - в появлении внутри система множества элементов, подструктур, для которых привычный режим функционирования стал в силу ряда обстоятельств недопустимым.

Скрытая угроза - это неосознаваемые системой в режиме реального времени входные данные, угрожающие ее безопасности.

В информационной войне наибольший приоритет отдается скрытым угрозам, так как именно они позволяют взращивать внутренние угрозы и целенаправленно управлять системой извне/

# Киберпреступность: понятие, история развития и расследования.

Парадокс развития человечества заключается в том, что на протяжении всего своего развития человек использовал, накапливал, передавал информацию. Непрерывный процесс информатизации общества охватывает все сферы деятельности человека и государства: от решения проблем национальной безопасности, здравоохранения и управления транспортом до образования, финансов, и даже просто межличностного общения. По мере развития технологий электронных платежей, «безбумажного» документооборота, серьезный сбой локальных сетей может парализовать работу целых корпораций и банков, что может привести к значительному материальному ущербу и колоссальным убыткам.

История киберпреступлений - это новейшая история, которая касается всех нас. В настоящее время проблема киберпреступности переросла в масштабы мирового сообщества.

Согласно рекомендациям экспертов ООН термин **«киберпреступность»** охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети [2]. **Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде.**

Преступление, совершенное в киберпространстве - это противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ.[1]

Сегодня киберпреступность - масштабная проблема, а вредоносные программы пишутся с целью незаконного получения денег. Развитие интернета стало одним из ключевых факторов, определивших эти перемены. Компании и отдельные пользователи уже не мыслят без него свою жизнь, и все больше финансовых операций проводится через интернет. Киберпреступники осознали, какие огромные возможности для «зарабатывания» денег с помощью вредоносного кода появились в последнее время, и многие из нынешних вредоносных программ написаны по заказу или с целью последующей продажи другим преступникам.

*Конвенция Совета Европы* говорит о четырех типах компьютерных преступлений, определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем[2]:

**незаконный доступ** - ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);

**незаконный перехват** - ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);

**вмешательство в данные** - ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);

**вмешательство в систему** - ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

На рисунке приведена классификация киберпреступлений.



Появление киберпреступности можно отсчитывать с момента появления компьютера, так называемой эпохи ЭВМ.

**Историю киберпреступлений можно разделить на два периода: первый - с момента создания первой ЭВМ до 1990 года и с 1990 года по настоящий момент времени.** Почему именно 1990 год ? Дело в том. что начиная с 1990 года интернет начал распространяться по миру с огромной скоростью.

Первое упоминание об использовании компьютера с целью совершения преступления было обнародовано в 1960-х годах, когда компьютеры представляли собой большие универсальные компьютеры, так называемые ЭВМ. После Второй мировой войны в 1946 году несколько компаний начали работать над коммерческими ЭВМ. и к 1951 году UNIVAC выпускает первый коммерческий компьютер, созданный в Соединённых Штатах, и третий коммерческий компьютер в мире (после германского Z4 и британского Ferranti Mark 1). который не предназначался для использования в научных исследованиях по разработке оружия. Первый экземпляр UNIVAC был официально продан Бюро переписи населения США. Всего за период с 1951 по 1958 год было создано 46 экземпляров UNIVAC. Они были установлены в правительственных учреждениях, частных корпорациях и в трех университетах США.

Электронные вакуумные лампы выделяли большое количество тепла, поглощали много электрической энергии, были громоздкими, дорогими и ненадежными. Компьютеры первого поколения, построенные на вакуумных лампах, обладали низким быстродействием и невысокой надежностью. В 1947 голу сотрудники американской компании «Белл» Уильям Шокли. Джон Бардин и Уолтер Бреттейн изобрели транзистор. Транзисторы выполняли тс же функции, что и электронные лампы, но использовали электрические свойства полупроводников. По сравнению с вакуумными трубками транзисторы занимали в 200 раз меньше места и потребляли в 100 раз меньше электроэнергии. В то же время появляются новые устройства для организации памяти компьютеров - ферритовые сердечники. С изобретением транзистора и использованием новых технологий хранения данных в памяти появилась возможность значительно уменьшить размеры компьютеров, сделать их более быстрыми и надежными, а также значительно увеличить емкость памяти компьютеров.

В 1954 году' компания Texas Instruments объявила о начале серийного производства транзисторов, а в 1956 году ученые Массачусетского технологического института создали первый, полностью построенный на транзисторах компьютер ТХ-О.

В 60-е годы прошлого столетия появилось третье поколение ЭВМ. в которых впервые стали использоваться интегральные схемы (микросхемы). В это же время появляется полупроводниковая память, которая и по сей день используется в персональных компьютерах в качестве оперативной. В эти годы производство компьютеров приобретает промышленный размах. Пробившаяся в лидеры фирма IBM первой реализовала семейство ЭВМ - серию полностью совместимых друг с другом компьютеров от самых маленьких, размером с небольшой шкаф (меньше тогда еще не делали), до самых мощных и дорогих моделей. Еще в начале 60-х появляются первые миникомпьютеры - небольшие маломощные компьютеры, доступные по цене небольшим фирмам или лабораториям. Миникомпьютеры представляли собой первый шаг на пути к персональным компьютерам, пробные образцы которых были выпущены только в середине 70-х голов. Вместе со стремительным развитием компьютерной сферы начинает свое развитие киберпреступность.

Но компьютерная преступность 1960-х и 1970-х годов отличалась от киберпреступности сегодня. Во-первых. в то время еще не появился Интернет, во-вторых. ЭВМ не были объединены в сеть. В 1960 голу' типичная ЭВМ стоила несколько миллионов долларов, занимала площадь одной комнаты и требовала специальной системы кондиционирования воздуха, чтобы компьютер не сгорел. В то время только определенный круг исследователей и ученых могли использовать ЭВМ в своей работе. Ограниченное использование ЭВМ и отсутствие соединения с другими компьютерами резко сокращало шансы совершения компьютерных преступлений, и если таковые совершались, то только людьми, которые обслуживали ЭВМ. Все преступления того времени сводились к преступлениям, связанным с финансовыми вложениями в ЭВМ. Это продолжалось до появления и всемирного распространения сети Интернет, что открыло новые возможности для преступников.

Историю киберпреступлений можно рассматривать в рамках истории развития хакерства.

***Хакер*** - это высококвалифицированный ИТ-специалист, человек, который понимает тонкости работы ЭВМ.

Различают два вида IT-xaкepoв:«White hat» и «Black hat». «Black hat» называют киберпреступников, тогда как «White hat» - прочих специалистов по информационной безопасности (в частности специалистов, работающих в крупных IT- компаниях) или исследователей ГГ-систем, не нарушающих закон.

В таблице выделены основные периоды истории существования хакерства, приведены их краткие характеристики.

|  |  |
| --- | --- |
| **Период** | **Характеристика** |
| 1960-е гг.: Зарождение хакерства | Первые компьютерные хакеры появились в Массачусетском технологическом институте (MIT).  Некоторые члены группы обращают свой пытливый ум на новый университетский компьютер и начинают манипулировать с программами. |
| 1970-е гг.: Телефонные фрикеры и Cap'nCrunch | Фрикеры взламывают местные и международные телефонные сети, чтобы звонить бесплатно. «Отец» фрикеров - участник войны во Вьетнаме Джон Дрэйпер (известный как Cap'nCrunch) - обнаружил, что игрушечный свисток-сувенир, который он нашел в коробке овсяных хлопьев Cap'nCrunch, издает звук с частотой 2600 герц, совпадающей с частотой электрического сигнала доступа в телефонную сеть дальней связи AT&T. Он построил первую «голубую коробку» BlueBox со свистком внутри, который свистел в микрофон телефона, позволяя делать бесплатные звонки. |
| 1980 г.: Хакерские доски сообщений и сообщества хакеров | Телефонные фрикеры начинают заниматься компьютерным хакерством, возникают первые системы электронных досок объявлений (BBS), предшественников групп новостей Usenet и электронной почты. BBS с такими названиями, как «SherwoodForest» и «Catch-22», становятся местами встреч хакеров и фрикеров, обмена опытом по краже паролей и номеров кредитных карт. Начинают формироваться хакерские группы. Первыми были «LegionofDoom» в США и «ChaosComputerClub» в Германии |
| 1983 г.: Детские игры | Первый фильм про хакеров «Военные игры» («WarGames») представил широкой общественности это явление. Главный персонаж - хакер - проникает в некий компьютер производителя видеоигр, который оказывается боевым симулятором ядер- ного конфликта, принадлежащего военным. В результате возникает реальная угроза ядерной войны, и военные переходят в режим «DefCon 1» (DefenseCondition 1 - высшая степень состояния боеготовности). Начинает формироваться образ хакера- кибергероя (и антигероя).  В том же году были арестованы 6 подростков, называвших себя «бандой 414». В течение 9 дней они взломали 60 компьютеров, среди которых машины Лос- Аламосской лаборатории ядерных исследований. |
| 1984г.: Хакерские журналы | Регулярно начал публиковаться хакерский журнал «2600». Редактор Эммануил Голдштейн (настоящее имя Эрик Корли) взял псевдоним от главного героя произведения Джоржа Оруэла «1984». Название журналу, как легко заметить, дала свистулька первого фрикера Cap'nCrunch. 2600, а также вышедший годом раньше онлайновый журнал «Phrack» публиковали обзоры и советы для хакеров и фрикеров. |
| 1986г.: За использование компьютера - в тюрьму | Обеспокоенный нарастанием количества взломов корпоративных и государственных компьютеров. Конгресс США принял «Соmputer Fraudand Abuse Act», который признал взлом компьютеров преступлением. Однако на несовершеннолетних он не распространялся. |
| 1988г.: Червь Морриса | Первый значительный ущерб от вредоносной программы. Саморазмножающаяся программа студента Корнельского университета Роберта Морриса вывела из строя около 6000 университетских и правительственных компьютеров по всей Америке, причинив огромный ущерб. |

**Второй этап** развития компьютерных преступлений начинается с середины 90-х годов прошлого столетия, это был период, когда Интернет распространялся со стремительной скоростью. Это было время, когда персональные компьютеры и Интернет становятся более доступными для всеобщего использования. В декабре 1995 года, по некоторым оценкам, было зарегистрировано 16 миллионов пользователей Интернета во всем мире, а уже к маю 2002 года эта цифра возросла до 580 миллионов, что составляло почти 10 процентов от общего населения планеты (NUA, 2003). Нужно отметить, что распространение Интернета по миру было неравномерно, например, более 95 процентов из общего числа Интернет-соединений располагались в США, Канаде, Европе, Австралии и Японии. Именно в это время в историю преступлений был введен новый вид преступлений, который носил название «Взлом».

На начальном этапе развития киберпреступлений очень часто используется термин «Взлом», хотя позже взлом будет определен как одно из преступлений, входящее в понятие киберпреступления. Именно взлом характеризует противозаконные действия хакеров. История развития хакерства в период с 1990 г. до наших дней приведена в таблице.

|  |  |
| --- | --- |
| **Период** | **Характеристика** |
| 1990 г.: Операция Sundevil | В 14 городах США прошла массовая облава на хакеров, обвиняемых в воровстве номеров кредитных карт и взломе телефонных сетей. Арестованные активно дают друг на друга показания в обмен на судебный иммунитет. По хакерским сообществам нанесен сильный удар. |
| 1993 г.: Зачем покупать машину, когда можно взломать? | Во время викторины-розыгыша автомобилей в прямом эфире на одной из радиостанций хакер в бегах Кевин Паулсен и двое его друзей так заблокировали телефонную сеть, что на радио проходили звонки только от них. Так они выиграли два автомобиля «Порше», турпоездки и 20 000 долларов.  Состоялся первый DefCon в Лас-Вегасе - самый крупный ежегодный съезд хакеров. Изначально DefCon планировался как разовая встреча, посвященная прощанию с BBS. Впоследствии мероприятие стало ежегодным. |
| 1994 г.: Хакерские утилиты перемещаются в веб | Появление браузера Netscape Navigator делает веб более удобным для просмотра и хранения информации, чем BBS. Хакеры со своими программами, утилитами, советами и технологиями переезжают с досок объявлений на веб-сайты. Все это богатство становится общедоступным. |
| 1995 г.: Пойманы Кевин Митник и Владимир Левин | Главный серийный киберпреступник - неуловимый Кевин Митник - наконец пойман ФБР. Судебные разбирательства длятся 4 года. Российский хакер - 30-летний Владимир Левин - крадет из американского Citibank 10 миллионов долларов. Его ловят и передают США. Приговор - 3 года тюремного заключения. Из похищенного возвращено все, кроме 400 000 долларов. |
| 1997г.: Взломы AOL | Свободно распространяемая хакерская программа с издевательским названием «AOHell» («America-On-Hell») стала кошмаром для AmericaOnline - крупнейшего интернет-провайдера. С ее помощью даже самый непродвинутый пользователь мог подкладывать многомегабайтные почтовые бомбы в e-mail-сервисы AOL и обрушивать потоки спама в чатах. |
| 1998 г.: Культ хакерства и израильская группа | Хакерская команда «Культ мертвой коровы» (CultoftheDeadCow) создает программу «BackOrifice» («Черный ход») для взлома Windows 95/98. Эта мощное средство захвата контроля над удаленной машиной через засланную троянскую утилиту. Программа представлена на съезде DefCon. |
| 2000 г.: В обслуживании отказано | На пике популярности распределенные атаки типа «Отказ от обслуживания» (denial-of-service или DDoS-атаки). Под их натиском падают крупнейшие сайты eBay, Yahoo!, CNN.com, Amazon и другие. Некие хакеры крадут из корпоративной сети Microsoft и публикуют исходные коды последних версий Windows и Office. |
| 2001 г.: DNS-атаки | Жертвой масштабного взлома DNS-серверов становятся сайты Microsoft. Корпорация проявляет чудеса нерасторопности. Многие ее сайты остаются недоступны для миллионов пользователей от нескольких часов до двух суток. |
| 2009 г.: Hacker-pro | Хакеры, обучавшиеся Hacker-pro, захватыают компьютеры всего мира, никто лучше них не делает фейки. Hacker-pro создали свой словарь брута, подбирающий пароль за несколько секунд, взлом всего за пару минут, теперь это возможно блогодаря Hacker-pro. |

Киберпреступность представляет собой не только техническую и правовую, но и социальную проблему, эффективное решение которой требует, прежде всего, системного подхода к разработке основ обеспечения безопасности жизненно важных интересов гражданина, общества и государства в киберпространстве.

По механизму и способам совершения преступления в сфере компьютерных технологий специфичны, имеют высокий уровень латентности. Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Рассматриваемое правонарушение имеет очень высокую латентность, которая, по различным данным, составляет 85-90% . Более того, факты обнаружения незаконного доступа к информационным ресурсам на 90% носят случайный характер [5]. Эти данные свидетельствуют о том, что работники правоохранительных органов зачастую просто не понимают, как расследовать данные преступления и как доказывать их в суде. Отсюда невозможность качественно проводить расследование, традиционные методы организации и планирования расследования не срабатывают в данных условиях, необходимо повышать эффективность правоохранительной деятельности, повышать уровень требовательности к уровню профессионализма сотрудников правоохранительных органов, их морально деловых качеств. Нельзя допускать их формального отношения к отчетности о результатах борьбы с компьютерной преступностью.

Еще одной проблемой, с которой зачастую сталкиваются следователи при расследовании преступлений в сфере компьютерных технологий, является установление факта совершения преступления. Это связано с тем, что зачастую компьютерные преступления совершаются в так называемом «киберпространстве», они не знают границ, очень часто преступления совершаются, не выходя из дома, с помощью своего персонального компьютера. Кроме того, незаконное копирование информации чаще всего остается необнаруженным, введение в компьютер вируса обычно списывается на непреднамеренную ошибку пользователя, который не смог его «отловить» при общении с внешним компьютерным миром. Да и отношение пострадавших к совершенному против них посягательству не всегда адекватно. Вместо того, чтобы сообщить правоохранительными органам о факте незаконного вмешательства в компьютерную систему, пострадавшие не торопятся этого делать, опасаясь подрыва деловой репутации. Обычно, в качестве потерпевшей стороны от компьютерных преступлений выступают локальные сети, серверы, физические лица.

Следует подчеркнуть, что профессиональные компьютерные преступники под объектом преступления выбирают локальные сети и серверы крупных компаний, в свою очередь «дилетанты» посягают на информацию компьютеров физических лиц и реже «ломают» провайдеров Интернет услуг, как правило, для «бесплатного» доступа в Интернет.

Примечателен тот факт, что потерпевшая сторона, в лице крупных корпораций, являющаяся собственником системы, неохотно сообщает (если сообщает вообще) в правоохранительные органы о фактах совершения компьютерного преступления. А поскольку они составляют большинство, то именно этим можно объяснить высокий уровень латентности компьютерных преступлений.

Кроме того, в раскрытии факта совершения преступления очень часто не заинтересованы должностные лица, в обязанности которых входит обеспечение компьютерной безопасности. Признание факта несанкционированного доступа в подведомственную им систему ставит под сомнение их профессиональную квалификацию, а несостоятельность мер по компьютерной безопасности, принимаемых руководством, может вызвать серьезные внутренние осложнения. Банковские служащие, как правило, тщательно скрывают обнаруженные ими преступления, которые совершены против компьютеров банка, так как это может пагубно отразиться на его престиже и привести к потере клиентов. Некоторые жертвы боятся серьезного компетентного расследования, потому что оно может вскрыть неблаговидную или даже незаконную механику ведения дел.

Есть еще одна проблема, связанная с эффективность расследования компьютерных преступлений и доведения их до суда. Это общественное мнение, которое не считает компьютерные преступления серьезным преступлением вследствие того, что компьютерные преступники, даже если расследование доведено до конца и вынесен приговор суда, отделываются легкими наказаниями, зачастую - условными приговорами. Отсюда - правовой нигилизм, с одной стороны преступников, которые чувствуют себя безнаказанно, а с другой стороны, потерпевших, которые не хотят обращаться в правоохранительные органы с заявлениями о несанкционированном доступе, потому что понимают, что должного наказания для преступников они все равно не добьются.

Можно выделить следующие факторы, влияющие на решение потерпевшей стороны не обращаться в правоохранительные органы по факту совершения компьютерного преступления:

1. Некомпетентность сотрудников правоохранительных органов в вопросе установления самого факта совершения компьютерного преступления.

2. Учитывая, что в случае уголовного расследования убытки от расследования могут оказаться выше суммы причиненного ущерба, возмещаемого в судебном порядке, многие организации предпочитают ограничиваться разрешением конфликта своими силами, что нередко завершается принятием мер, не исключающих рецидив компьютерных преступлений.

3. Боязнь подрыва собственного авторитета в деловых кругах и как результат этого — потеря значительного числа клиентов. Эго обстоятельство особенно характерно для банков и крупных финансово-промышленных организаций, занимающихся широкой автоматизацией своих производственных процессов.

4. Неминуемое раскрытие в ходе судебного разбирательства системы безопасности организации, что нежелательно для нее.

5. Боязнь возможности выявления в ходе расследования преступления собственного незаконного механизма осуществления отдельных видов деятельности и проведения финансово-экономических операций.

6. Выявление в ходе расследования компьютерного преступления причин, способствующих его совершению, может поставить под сомнение профессиональную пригодность (компетентность) отдельных должностных лиц, что в конечном итоге приведет к негативным для них последствиям.

7. Правовая и законодательная неграмотность подавляющего большинства должностных лиц в вопросах рассматриваемой категории понятий.

Часто организации имеют весьма далекое представление о реальной ценности информации, содержащейся в их компьютерных системах. Обычно ценность определяется стоимостью ее создания или ее конкурентоспособностью, причем все чаще предпочтение отдается последнему. Диапазон содержащихся в ней данных простирается от производственных секретов и планов до конфиденциальной информации и списков клиентов, которые преступник может использовать с целью шантажа или в других целях. Эта информация имеет различную ценность для собственника и того лица, которое пытается ее получить. Непосредственная стоимость информации оценивается и с учетом затрат на ее сбор, обработку и хранение, а также рыночной ценой. В то же время на нее влияют и некоторые обстоятельства, связанные с совершением компьютерных преступлений. Необходимо также особо подчеркнуть, что успех расследования уголовных дел в сфере компьютерных технологий зависит от правильной организации и планирования.

**Пример:**

В июне 2016 г. правительство США обнаружило, что компьютерная сеть Национального комитета Демократической партии США была дважды взломана: летом 2015 г. и в апреле 2016 г. Атаки осуществили хакерские группировки Cozy Bear и Fancy Bear. Преступники получили доступ к чатам и почте политиков демократического крыла, а также нашли их досье на кандидата в президенты от республиканцев Дональда Трампа (Donald Trump).

Поскольку хакеры не заинтересовались финансовыми данными демократов, цель взлома определили не как обогащение, а как шпионаж. Самым вероятным кандидатом на роль кибершпиона США посчитали Россию, которая отрицала какую-либо причастность к атакам. В ходе дискуссии некоторые американцы заговорили о том, что нельзя обвинять другие страны в кибершпионаже, когда Вашингтон тоже постоянно им занимается[12].

Переписка DNC была опубликована 23 июля на сайте WikiLeaks. В утечке оказались более 19 тыс. электронных писем и более 8 тыс. документов из служебной переписки ключевых функционеров DNC (финансового директора Джордона Каплана, директора по коммуникациям Луиса Миранды и ряда других) в период с января 2015 по май 2016 года.

Президент США Барак Обама в интервью NBC не исключил , что российские хакеры могут быть причастны к взлому серверов Демократической партии США и утечке переписки партийного руководства.

Ппресс-секретарь президента России Дмитрий Песков ответил на обвинения демократов США опровержением о какой-либо причастности властей или официальных лиц России к хакерским атакам[13].

**Заявление:**

Хакеры, взломавшие Демократическую партию США, могли намеренно оставить «российский след». Об этом рассказали представители американской разведки агентству [Reuters](http://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Reuters). Эксперты на условиях анонимности рассказали, что хакеры намеренно хотели выставить себя русскими, оставляя кириллические символы в метаданных и прекращая деятельность в религиозные и государственные праздники [России](http://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8).

Источники Reuters в американском разведсообществе рассказали, почему нежелательно обвинять Россию в причастности к последним хакерским атакам. По их мнению, это может привести к глобальной конфронтации с Москвой[[14]](http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D0%B8%D0%BA%D1%82%D1%8B_:_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F#cite_note-13). если Белый дом публично обвинит в хакерстве российские спецслужбы, то от него потребуют раскрыть доказательства их причастности, которые основывают на информации из совершенно секретных источников и совершенно секретных методах. Ответные действия США против России в киберпространстве приведут, по мнению собеседников Reuters из разведсообщества, к быстрой эскалации взаимных контрмер. Они опасаются, что в худшем случае российские хакеры проникнут в американские энергосистемы, финансовые организации и другие значимые объекты инфраструктуры.

Президент РФ [Владимир Путин](http://www.tadviser.ru/index.php/%D0%92%D0%BB%D0%B0%D0%B4%D0%B8%D0%BC%D0%B8%D1%80_%D0%9F%D1%83%D1%82%D0%B8%D0%BD) считает, что взлом Национального комитета Демократической партии США и последующая публикация похищенных электронных писем и документов принесли несомненную пользу обществу, однако Россия не имеет к этому никакого отношения. «Разве имеет значение, кто взломал? Главное – предоставленная обществу информация, – заявил президент в интервью журналистам Bloomberg 2 сентября 2016 года. – Не стоит отвлекать внимание общественности от истинной проблемы, поднимая малосущественные вопросы, связанные с поиском тех, кто это сделал. Однако я повторяю еще раз, что мне ничего не известно об этом, и на государственном уровне Россия не имеет к этому никакого отношения».

В соответствии с действующим [уголовным законодательством Российской Федерации](https://ru.wikipedia.org/wiki/%D0%A3%D0%9A_%D0%A0%D0%A4) под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные среде.

Данная группа посягательств являются [институтом](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BF%D1%80%D0%B0%D0%B2%D0%B0) особенной части уголовного законодательства, [ответственность](https://ru.wikipedia.org/wiki/%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%B0%D1%8F_%D0%BE%D1%82%D0%B2%D0%B5%D1%82%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C) за их совершение предусмотрена гл. 28 УК РФ. В качестве самостоятельного института впервые выделен [УК РФ](https://ru.wikipedia.org/wiki/%D0%A3%D0%9A_%D0%A0%D0%A4) [1996 года](https://ru.wikipedia.org/wiki/1996_%D0%B3%D0%BE%D0%B4). и относится к субинституту «[Преступления против общественной безопасности и общественного порядка](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B2_%D0%BE%D0%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%B8_%D0%BE%D0%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D1%80%D1%8F%D0%B4%D0%BA%D0%B0&action=edit&redlink=1)». Видовым [объектом](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%8A%D0%B5%D0%BA%D1%82_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) рассматриваемых преступлений являются [общественные отношения](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5_%D0%BE%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D1%8F), связанные с безопасностью информации и систем обработки информации с помощью [ЭВМ](https://ru.wikipedia.org/wiki/%D0%AD%D0%92%D0%9C).

По [УК РФ](https://ru.wikipedia.org/wiki/%D0%A3%D0%9A_%D0%A0%D0%A4) преступлениями в сфере компьютерной информации являются: [неправомерный доступ к компьютерной информации](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%BC%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%D0%BA_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (ст. 272 УК РФ), [создание, использование и распространение вредоносных компьютерных программ](https://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5,_%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B8_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B2%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D1%8B%D1%85_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC&action=edit&redlink=1) (ст. 273 УК РФ), [[нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей]] (ст. 274 УК РФ).

Общественная опасность противоправных действий в области [электронной техники](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D0%BA%D0%B0) и [информационных технологий](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8) выражается в том, что они могут повлечь за собой нарушение деятельности [автоматизированных систем управления](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) и контроля различных объектов, серьёзное нарушение работы [ЭВМ](https://ru.wikipedia.org/wiki/%D0%AD%D0%92%D0%9C) и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) и [информационных ресурсов](https://ru.wikipedia.org/w/index.php?title=%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B9_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81&action=edit&redlink=1), иные формы незаконного вмешательства в [информационные системы](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B), которые способны вызвать тяжкие и необратимые последствия, связанные не только с [имущественным ущербом](https://ru.wikipedia.org/wiki/%D0%98%D0%BC%D1%83%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D1%83%D1%89%D0%B5%D1%80%D0%B1), но и с [физическим вредом](https://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B2%D1%80%D0%B5%D0%B4&action=edit&redlink=1) людям.

[Неправомерный доступ к компьютерной информации](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%BC%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%D0%BA_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (ст. 272 УК РФ), а также [Создание, использование и распространение вредоносных компьютерных программ](https://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5,_%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B8_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B2%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D1%8B%D1%85_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC&action=edit&redlink=1) (ст. 273 УК РФ) совершаются только путём действий, в то время как [[нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей]] (ст. 274 УК РФ) — путём как действий, так и бездействием.

[Неправомерный доступ к компьютерной информации](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%BC%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%D0%BA_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) и [нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети](https://ru.wikipedia.org/w/index.php?title=%D0%9D%D0%B0%D1%80%D1%83%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB_%D1%8D%D0%BA%D1%81%D0%BF%D0%BB%D1%83%D0%B0%D1%82%D0%B0%D1%86%D0%B8%D0%B8_%D0%AD%D0%92%D0%9C,_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D0%AD%D0%92%D0%9C_%D0%B8%D0%BB%D0%B8_%D0%B8%D1%85_%D1%81%D0%B5%D1%82%D0%B8&action=edit&redlink=1) сформулированы как [преступления](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) с [материальным составом](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%81%D1%82%D0%B0%D0%B2_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F), а [создание либо использование вредоносных программ для ЭВМ](https://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BB%D0%B8%D0%B1%D0%BE_%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B2%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC_%D0%B4%D0%BB%D1%8F_%D0%AD%D0%92%D0%9C&action=edit&redlink=1) — с [формальным](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%81%D1%82%D0%B0%D0%B2_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F). В качестве последствий в ст. 272 и 274 УК указываются: уничтожение, модификация, блокирование либо копирование [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F), нарушение работы [ЭВМ](https://ru.wikipedia.org/wiki/%D0%AD%D0%92%D0%9C) или системы ЭВМ, причинение существенного вреда и т. п.

В России борьбой с преступлениями в сфере информационных технологий занимается [Управление «К» МВД РФ](https://ru.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%C2%AB%D0%9A%C2%BB) и отделы «К» региональных управлений внутренних дел, входящие в состав Бюро специальных технических мероприятий МВД РФ.

# Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

В январе 2013 г. президент Владимир Путин подписал указ о создании в России системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, расположенные в стране и в дипломатических представительствах и консульских учреждениях России за рубежом.

Ее ключевыми задачами, в соответствии с указом президента, должно стать прогнозирование ситуаций в области обеспечения [[информационной безопасности, обеспечение взаимодействия владельцев ИТ-ресурсов при решении задач, связанных с обнаружением и ликвидацией компьютерных атак, с операторами связи и другими организациями, осуществляющими деятельность по защите информации. В список задач системы также входит оценка степени защищенности критической ИТ-инфраструктуры от компьютерных атак и установление причин таких инцидентов.

Организацию работ по созданию государственной анти-хакерской системы Путин поручил ФСБ.

В декабре 2014 года президент Владимир Путин утвердил концепцию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

В марте 2015 года ФСБ опубликовала выписку из этого документа, содержащую данные о том, как будет устроена эта система.

В «Концепции» перечислены 12 функций по обеспечению информационной безопасности интернет-ресурсов, возложенных на Систему. Среди них:

* выявление признаков проведения компьютерных атак,
* разработка методов и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;
* формирование детализированной информации об информационных ресурсах РФ, находящихся в зоне ответственности Системы (то есть ресурсов органов власти);
* прогнозы в области обеспечения ИБ Российской Федерации;
* организация и взаимодействие с правоохранительными органами и другими госорганами, владельцами информационных ресурсов Российской Федерации, операторами связи, интернет-провайдерами и иными заинтересованными организациями на национальном и международном уровнях в области обнаружения компьютерных атак и установления их источников;
* организация и проведение научных исследований в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак и др.

Согласно документу, система представляет собой единый централизованный территориально-распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган власти, уполномоченный в области обеспечения безопасности критической инфраструктуры РФ и орган власти, уполномоченный в области создания и обеспечения функционирования системы.

Под «средствами» в концепции подразумеваются, главным образом, технологические решения, а под «силами» - специальные подразделения и сотрудники со стороны федерального органа власти, ответственного за систему, а также операторов связи и других организаций, осуществляющих лицензируемую деятельность в сфере защиты информации.

Основной организационно-технической составляющей системы являются центры обнаружения, предупреждения и ликвидации последствий компьютерных атак, которые будут подразделяться по территориальному и ведомственному признакам. В частности, будет организован главный центр, региональные, территориальные центры системы, а также центры госорганов и корпоративные центры. Функционирование последних будет обеспечиваться организациями, их создавшими.

В составе системы также функционирует созданный в ФСБ Национальный координационный центр по компьютерным инцидентам, который организует и осуществляет обмен информацией о них с юрлицами, владеющими объектами критической ИТ-инфраструктуры РФ, операторами связи, обеспечивающими взаимодействие объектов критической ИТ-инфраструктуры, а также с иностранными госорганами и другими организациями, работающими в области реагирования на кибер-инциденты.

Основными функциями системы, указано в концепции, является выявление признаков проведения компьютерных атак, определение их источников и другой связанной информации, прогнозирование ситуации в области обеспечения информационной безопасности РФ, сбор и анализ информации о компьютерных атаках в отношении информационных ресурсов РФ, осуществление мероприятий по оперативному реагированию на атаки и ликвидации их последствий и др.

Также рамках системы планируется организовать взаимодействие с правоохранительными и другими госорганами, владельцами информационных ресурсов РФ, операторами связи и интернет-провайдерами на национальном и международном уровнях. Оно будет включать обмен информацией о выявленных компьютерных атаках и обмен опытом в сфере в сфере выявления и устранения уязвимостей ПО и оборудования и реагирования на компьютерных инциденты.

Для функционирования системы планируется создать соответствующую законодательную базу, определить порядок фиксации и обмена информацией о компьютерных атаках, деятельности субъектов системы в области обнаружения, предупреждения и ликвидации последствий атак.

Возможен подход на основе классификации информационных активов организаций по степени их ценности, важности для обеспечения управления государством и сохранения знаний, необходимых для развития страны. Дифференцированные требования к защите классифицированных таким образом информационных активов можно установить законом, возложив ответственность на сами ведомства, в чьём ведении информационные ресурсы находятся – без привлечения организаций, аккредитованными ФСТЭК России.

В этом случае появится возможность создания произвольной структуры ГосСОПКА (сегменты системы по министерствам. ведомствам, организациям, субъектам РФ) и существенно удешевить разработку стоимость работ (не потребуется создавать свои программно-технические средства). Надёжность не пострадает – изоляция важнейших элементов IT-инфраструктуры будет безопаснее, чем подключение через доверенные средства.

Органический недостаток такого подхода – изоляция части системы, что влечёт снижение оперативности работы системы и неудобства для пользователей.

Альтернативный подход состоит в поиске критических мест инфраструктуры и их защите доверенными средствами. В этом случае классификация информационных ресурсов по степени их важности неактуальна, но необходима (или, как минимум, крайне желательна) отечественная программно-техническая платформа.

Преимущества второго подхода значительны. Во-первых, отсутствует необходимость изоляции сегментов системы и создаётся единое защищённое информационное пространство с «прозрачным» администрированием. Как следствие, повышается оперативность, улучшается контроль всех процессов. Во-вторых, защита всей инфраструктуры страны обеспечивается отечественными программно-техническими средствами с максимально высоким уровнем защиты.

Расплата за эти преимущества – высокая стоимость проекта и большое время разработки.

**Раздел 3. Методы и средства защиты.**

В соответствии со статьей 8 Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности»Президент Российской Федерации устанавливает компетенцию федеральных органов исполнительной власти в области обеспечения безопасности, руководство деятельностью которых он осуществляет и решает в соответствии с законодательством Российской Федерации вопросы, связанные с обеспечением защиты информации и государственной тайны.

Соответствующими указами Президентом определены федеральные органы исполнительной власти, реализующие полномочия по защите информации:

**Федеральная служба то техническому и экспортному контролю Российской Федерации** (ФСТЭК России) - Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

* противодействия иностранным техническим разведкам на территории Российской Федерации;
* обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения государственными органами и организациями.

ФСТЭК России осуществляет методическое руководство деятельностью государственных органов и организаций в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации.

**Федеральная служба безопасности Российской Федерации** (ФСБ России) - Указ Президента РФ от 11.08.2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации».

Основными задачами ФСБ России в области защиты информации являются:

* обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;
* формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;
* организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

Различие компетенций вышеперечисленных органов исполнительной власти заключается в следующем:

ФСТЭК России формирует требования и производит контроль мероприятий по защите информации **некриптографическими методами** (разграничение прав пользователей, защита информации от побочных электромагнитных излучений, защита речевой информации и др.);

ФСБ России формирует требования и производит контроль мероприятий по защите информации **криптографическими методами** (защита каналов связи, электронная подпись).

Защита информации некриптографическими методами является наиболее массовым видом при создании защищенных информационных систем.

В соответствии со статьей 12 федерального закона «О безопасности» органы государственной власти субъектов Российской Федерации и органы местного самоуправления в пределах своей компетенции **обеспечивают исполнение законодательства Российской Федерации в области обеспечения безопасности**.

 Основным документом, определяющим порядок создания системы защиты информации и проведения контроля, является «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденное Постановлением Совета Министров - Правительства Российской Федерации от 15.09.1993 № 912-51.

Организация работ по защите информации в органах исполнительной власти осуществляется их руководителями. Для организации и проведения работы по защите информации создаются специальные подразделения по защите информации (или штатные специалисты).

В органах исполнительной власти субъекта может циркулировать два вида информации подлежащей обязательной защите в соответствии с действующим законодательством:

**1. Информация, составляющая государственную тайну** (Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»).

**2. Конфиденциальная информация** (Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»), которая в свою очередь делится на несколько составляющих, наиболее часто встречающихся в исполнительных органах власти:

* персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу);
* служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с федеральными законами (служебная тайна – сведения, содержащие информацию ограниченного доступа, документы с пометкой «Для служебного пользования»).

Для вышеперечисленных видов информации должны в обязательном порядке применяться меры по защите информации.

Одна из основных целей защиты информации – это предотвращение ее утечки по техническим каналам.

В соответствии со статьей 16 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, обладатель информации, обязан обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

 Конкретные требования по защите информации, которые должен обеспечить обладатель информации, отражены в руководящих документах ФСТЭК и ФСБ России. Документы также делятся на ряд направлений:

* защита информации при обработке сведений, составляющих государственную тайну;
* защита конфиденциальной информации (в т.ч. персональных данных);
* защита информации в ключевых системах информационной инфраструктуры.

Конкретные требования по защите информации определены в руководящих документах ФСТЭК России.

При создании и эксплуатации государственных информационных систем (а это все информационные системы областных органов исполнительной власти) методы и способы защиты информации должны соответствовать требованиям ФСТЭК и ФСБ России.

Документы, определяющие порядок защиты конфиденциальной информации и защиты информации в ключевых системах информационной инфраструктуры имеют пометку «Для служебного пользования». Документы по технической защите информации, как правило, имеют гриф «секретно».

**Защитные меры** (см., например, ГОСТ ИСО/МЭК 13335) – это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов.

Эффективная безопасность обычно требует комбинации различных защитных мер для обеспечения заданных уровней безопасности при защите активов. Например, механизмы контроля доступа, применяемые к вычислительным средствам, должны подкрепляться аудитом, определенным порядком действий персонала, его обучением, а также физической защитой. Часть защитных мер может быть обеспечена внешними условиями, свойствами актива или может уже существовать в системе или организации.

Порядок выбора защитных мер очень важен для правильного планирования и реализации программы информационной безопасности. Защитная мера может выполнять много функций безопасности, и, наоборот, одна функция безопасности может потребовать нескольких защитных мер. Защитные меры могут выполнять одну или несколько из следующих функций: предотвращение; сдерживание; обнаружение; ограничение; исправление; восстановление; мониторинг; осведомление.

Некоторые защитные меры могут характеризовать позицию организации в области информационной безопасности. В связи с этим важно выбирать специфические защитные меры, не причиняющие ущерба культурной и социальной среде, в которой функционирует организация. Примеры таких специфических защитных мер: политики и процедуры; механизмы контроля доступа; антивирусное программное обеспечение; шифрование; цифровая подпись; инструменты мониторинга и анализа; резервный источник питания; резервные копии информации.

**Меры обеспечения ИБ** (или меры контроля в понятиях ГОСТ Р ИСО/МЭК 27001, или защитные меры в терминах ISO 13335-1) имеют разветвленную сложную структуру и состоят из организационных и программно-технических мер на верхнем уровне.

В свою очередь, **организационные меры** включают законодательные, административные и процедурные меры обеспечения ИБ. Законодательные меры включают в себя законы, стандарты, регламенты и другие нормативные документы.

Основой **административных мер**, осуществляемых руководством организации, является политика безопасности.

**Процедурные,** то есть реализуемые людьми, меры безопасности включают меры по: управлению персоналом; физической защите; поддержке работоспособности; реагированию на нарушения режима безопасности; планированию восстановительных работ.

**Способы защиты информации:**

1. **Препятствие** - создание на пути угрозы преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.
2. **Управление** - оказание управляющих воздействий на элементы защищаемой системы.
3. **Маскировка** - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника. (Сюда можно, в частности, отнести криптографические методы защиты ).
4. **Регламентация** - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов.
5. **Принуждение** - метод заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия обработки информации под угрозой ответственности (материальной, уголовной, административной)
6. **Побуждение** - метод заключается в создании условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

**Частные виды методов защиты информации:**

1. **Управление доступом** – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Управление доступом включает следующие функции зашиты:

* идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
* опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
* проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
* разрешение и создание условий работы в пределах установленного регламента;
* регистрацию (протоколирование) обращений к защищаемым ресурсам;
* реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

1. **Механизмы шифрования** – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.
2. **Противодействие атакам вредоносных программ** предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

****

**Средства защиты информации:**

1. **Физические средства** - механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.
2. **Аппаратные средства** - различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.
3. **Программные средства** - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.
4. **Организационные средства** - организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации.
5. **Законодательные средства** - нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности.
6. **Психологические (морально-этические средства)** - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

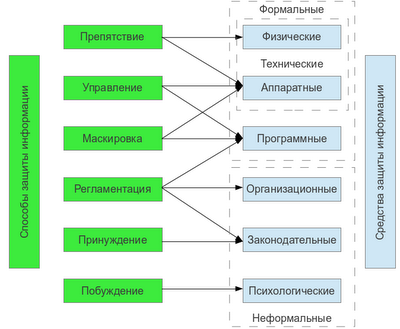


Рис.1.2. Классификация методов и средств защиты информации.

**Требования по защите информации**

**(РД АС от НСД, СВТ от НСД, МЭ, НДВ)**

На настоящее время защита информации на государственном уровне сконцентрирована вокруг вопросов обеспечения конфиденциальности информации. Тем не менее, современное развитие информатизации требует уделять больше внимания обеспечению таких свойств информации, как целостность и доступность. На практике же есть достаточно много форм деятельности, где доля конфиденциальной информации сравнительно мала. Например, для открытой информации приоритетными направлениями будет обеспечение целостности и доступности информации. Для платежных документов, отправляемых через системы дистанционного банковского обслуживания, наибольшую важность представляет целостность информации, так как если документ будет подделан, владелец может получить колоссальный финансовый ущерб. Следовательно, традиционный подход к защите информации с точки зрения обеспечения только конфиденциальности, требует существенной модернизации.

**Требования по защите информации.**

**Классификация АС**

Подавляющее большинство информации в современном мире обрабатывается в автоматизированных системах (АС). Следовательно, АС является «наиболее популярным» объектом защиты. Все действующие АС, обрабатывающие конфиденциальную информацию, соответственно, нуждающиеся в защите от НСД, классифицируются в соответствии с Руководящим документом Гостехкомиссиии России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации».

В соответствии с документом, классификация АС включает следующие этапы:

1. Разработка и анализ исходных данных.
2. Выявление основных признаков АС, необходимых для классификации.
3. Сравнение выявленных признаков АС с классифицируемыми.
4. Присвоение АС соответствующего класса защиты информации от НСД.

Исходными данными для классификации АС являются:

* Перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности.
* Перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий.
* Матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС.
* Режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

К числу определяющих признаков классификации АС относится следующее:

* наличие в АС информации различного уровня конфиденциальности;
* уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС - коллективный или индивидуальный.

Устанавливаются **9 классов защищённости АС от НСД** к информации, каждый класс характеризуется определённой минимальной совокупностью требований по защите. Классы подразделяются на 3 группы:

**III группа – классы 3Б и 3А.**

Классы соответствуют автоматизированным системам, в которых работает один пользователь, допущенный ко всей информации в АС, размещённой на носителях одного уровня конфиденциальности.

**II группа – классы 2Б и 2А.**

Классы данной группы соответствуют автоматизированным системам, в которых пользователи имеют одинаковые права доступа ко всей информации в АС, обрабатываемой или хранимой на носителях различного уровня конфиденциальности.

**I группа – классы 1Д, 1Г, 1В, 1Б и 1А.**

В этих автоматизированных системах одновременно обрабатывается или хранится информация разных уровней конфиденциальности. Не все пользователи имеют доступ ко всей информации в АС.

Интересно, что документ выделяет 4 подсистемы для обеспечения защиты от НСД:

* управления доступом;
* регистрации и учета;
* криптографическая;
* обеспечения целостности.

Более детально требования в зависимости от класса защищенности описаны в Руководящем документе Гостехкомиссиии России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации». Пересмотр класса защищенности АС производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен.

Если АС, классифицированная ранее, включается в состав вычислительной сети или системы и соединяется с другими техническими средствами линиями связи различной физической природы, образуемая при этом АС более высокого уровня классифицируется в целом, а в отношении АС нижнего уровня классификация не производится.

Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС, за исключением случаев их объединения посредством межсетевого экрана, когда каждая из объединяющихся АС может сохранять свой класс защищенности.

**Классификация СВТ**

Гостехкомиссия России, ныне ставшая ФСТЭК, разделила понятия АС и средств вычислительной техники (СВТ). Выделение СВТ в отдельную категорию обусловлено тем, что СВТ представляют собой компоненты при построении АС, то есть если СВТ не интегрированы в АС и не решают какой-то прикладной задачи, они не содержат пользовательской информации. Помимо этого, АС является более широким понятием, включающим в себя персонал, помещения, технологии обработки информации, полномочия пользователей системы.

Пример: ПЭВМ с установленной на ней операционной системой формально является СВТ. Но если ее поставить в конкретную комнату, закрепить за ней пользователя, выполняющего какую-то работу, - АС. Следует отметить, что средства защиты информации также относятся к СВТ.

СВТ - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[[8.3]](http://www.intuit.ru/studies/courses/2291/591/literature#literature.1.1).

СВТ классифицируются в соответствии с Руководящим документом Гостехкомиссиии России "СВТ. Защита от НСД к информации. Показатели защищенности от НСД"

Руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищённости от НСД к информации на базе перечня показателей защищённости и совокупности описывающих их требований.

Устанавливаются **7 классов защищённости СВТ от НСД** к информации, при этом самый низкий класс – седьмой, самый высокий – первый. Каждый класс разбит на 4 группы:

**I. 7 класс** – СВТ, которые были представлены к оценке, однако не удовлетворяют требованиям более высоких классов.

**II. 6 и 5 классы** – дискреционная защита.

**III. 4, 3 и 2 классы** – мандатная защита.

**IV. 1 класс** – верифицированная защита.

Требования ужесточаются с уменьшением номера класса.

Классы являются иерархически упорядоченными: каждый последующий класс содержит требования всех предыдущих. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

В общем случае требования предъявляются к следующим показателям защищённости:

Дискреционный принцип контроля доступа.

Мандатный принцип контроля доступа.

Очистка памяти.

Изоляция модулей.

Маркировка документов.

**Классификация межсетевых экранов.**

Наиболее распространенными средствами защиты сетей являются МЭ. Главная функция МЭ – экранирование сетевого трафика с целью предотвращения несанкционированного доступа между компьютерными сетями.

В качестве МЭ могут выступать маршрутизаторы, персональный компьютер или набор узлов, расположенные между надежными (например, внутренними) и ненадежными (например, Интернет) сетями и контролирующие весь трафик, который между ними проходит.

Эффективность МЭ обуславливается тем, что:

• все соединения проходят через МЭ (в противном случае, если есть альтернативный сетевой маршрут, эффективность сильно снижается);

• МЭ пропускают только санкционированный трафик;

• МЭ должен противостоять атакам против самого себя.

Преимущества МЭ

• МЭ ограничивает доступ к определенным службам (например, общий доступ к веб-узлу может быть разрешен, а к telnet - запрещен).

• МЭ – средство аудита. Они могут заносить в журнал информацию о любом проходящем трафике.

• МЭ обладают возможностями по оповещению о конкретных событиях.

Недостатки МЭ

• МЭ разрешают установку обычных соединений санкционированных приложений, но если приложение представляет собой угрозу, МЭ не сможет предотвратить ее реализацию (например, МЭ разрешают прохождение электронной почты на почтовый сервер, но не находит вирусов в сообщении).

• Эффективность МЭ зависит от правил, на соблюдение которых они настроены.

• МЭ не защищают от аутсайдеров.

• МЭ не предотвращают атаки, если трафик не проходит через них.

Согласно Руководящему документу «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» **Устанавливается пять классов защищенности МЭ.**

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

1.6. Требования, предъявляемые к МЭ, не исключают требований, предъявляемых к средствам вычислительной техники (СВТ) и АС в соответствии с руководящими документами Гостехкомиссии России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” и “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.

При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:   
- при обработке информации с грифом “секретно” - не ниже 3 класса;  
- при обработке информации с грифом “совершенно секретно” - не ниже 2 класса;  
- при обработке информации с грифом “особой важности” - не ниже 1 класса.

**Классификация ПО по НДВ.**

Недекларированные возможности - функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Реализацией недекларированных возможностей, в частности, являются программные закладки.

2.2. Программные закладки – преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

2.3. Функциональный объект – элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы.

В качестве функциональных объектов могут выступать процедуры, функции, ветви, операторы и т.п.

2.4. Информационный объект - элемент программы, содержащий фрагменты информации, циркулирующей в программе. В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т.п.

2.5. Маршрут выполнения функциональных объектов – определенная алгоритмом последовательность выполняемых функциональных объектов.

2.6. Фактический маршрут выполнения функциональных объектов – последовательность фактически выполняемых функциональных объектов при определённых условиях (входных данных).

Критический маршрут выполнения функциональных объектов – такой маршрут, при выполнении которого существует возможность неконтролируемого нарушения установленных правил обработки информационных объектов.

. Статический анализ исходных текстов программ – совокупность методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстов программ.

Динамический анализ исходных текстов программ – совокупность методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа.

1.1. Классификация распространяется на ПО, предназначенное для защиты информации ограниченного доступа.

1.2. Устанавливается четыре уровня контроля отсутствия недекларированных возможностей. Каждый уровень характеризуется определенной минимальной совокупностью требований.

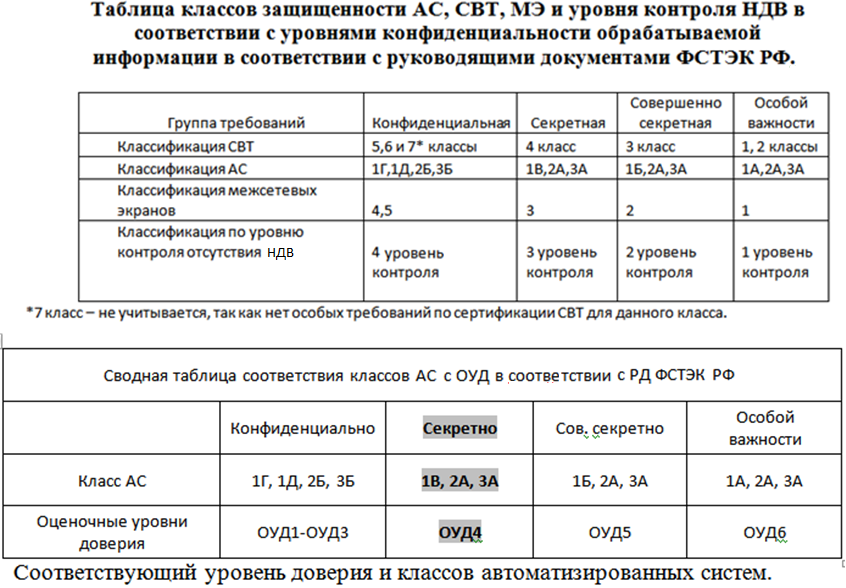
1.3. Для ПО, используемого при защите информации, отнесенной к государственной тайне, должен быть обеспечен уровень контроля не ниже третьего.

1.4. Самый высокий уровень контроля - первый, достаточен для ПО, используемого при защите информации с грифом «ОВ».

Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «CC».

Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом «C».

1.5 Самый низкий уровень контроля - четвертый, достаточен для ПО, используемого при защите конфиденциальной информации.



**Принципы построения защищенной АИС**

Задачи системы информационной безопасности

Система обеспечения информационной безопасности АИС должна решать следующие задачи с целью противодействия основным угрозам ИБ:

1. Управление доступом пользователей к ресурсам АИС.
2. Защита данных, передаваемых по каналам связи.
3. Регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности.
4. Контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы.
5. Обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ (в которых могут содержаться вредоносные закладки или опасные ошибки) и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов.
6. Контроль и поддержание целостности критичных ресурсов системы защиты; управление средствами защиты.

Различают внешнюю и внутреннюю безопасность АИС. *Внешняя безопасность* включает защиту АС от стихийных бедствий (пожар, землетрясение и т.п.) и от проникновения в систему злоумышленников извне. *Внутренняя безопасность* заключается в создании надежных и удобных механизмов регламентации деятельности всех ее законных пользователей и обслуживающего персонала.

**Меры противодействия угрозам безопасности**

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются на: законодательные (правовые), административные (организационные), процедурные и программно-технические.

К *законодательным мерам защиты* относятся действующие в стране нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Важное значение имеют стандарты в области защиты информации (в первую очередь, ме-ждународные). Среди этих стандартов выделяются «Оранжевая книга», рекомендации X.800 и «Общие критерии оценки безопасности информационных технологий» (Common Criteria for IT Security Evaluation).

«Оранжевая книга» — крупнейший базовый стандарт. В ней даются важнейшие понятия, определяются основные сервисы безопасности и предлагается метод классификации информационных систем по требованиям безопасности.

Рекомендации X.800 в основном посвящены вопросам защиты сетевых конфигураций. Они предлагают развитый набор сервисов и механизмов безопасности.

«Общие критерии» описывают 11 классов, 66 семейств и 135 компонентов функцио-нальных требований безопасности. Классам присвоены следующие названия:

Первая группа определяет элементарные сервисы безопасности:

1. FAU — аудит, безопасность (требования к сервису, протоколирование и аудит);
2. FIA — идентификация и аутентификация;
3. FRU — использование ресурсов (для обеспечения отказоустойчивости).

Вторая группа описывает производные сервисы, реализованные на базе элементарных:

1. FCO — связь (безопасность коммуникаций отправитель-получатель);
2. FPR — приватность;
3. FDP — защита данных пользователя;
4. FPT — защита функций безопасности объекта оценки.

Третья группа классов связана с инфраструктурой объекта оценки:

1. FCS — криптографическая поддержка (обслуживает управление криптоключами и крипто-операциями);
2. FMT — управление безопасностью;
3. FTA — доступ к объекту оценки (управление сеансами работы пользователей);
4. FTP — доверенный маршрут/канал;

Кроме этого «Общие критерии» содержат сведения о том, каким образом могут быть достигнуты цели безопасности при современном уровне информационных технологий и позволяют сертифицировать систему защиты (ей присваивается определенный уровень безопасности).

Осенью 2006 года в России был принят национальный стандарт ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология — Практические правила управления инфомационной безопасностью», соотвествующий международному стандарту ИСО 17799. Стандарт представляет собой перечень мер, необходимых для обеспечения информационной безопасности организации, включая действия по созданию и внедрению системы управления информационной безопасности, которая строится таким же образом и на тех же принципах, что и система менеджмента качества, и совместима с ней.

*Административные меры защиты* —меры организационного характера,регламентирующие процессы функционирования АИС, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают:

1. Подбор и подготовку персонала системы.
2. Организацию охраны и пропускного режима.
3. Организацию учета, хранения, использования и уничтожения документов и носителей с информацией.
4. Распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.д.).
   * составе административных мер защиты важную роль играет формирование программы работ в области информационной безопасности и обеспечение ее выполнения (для этого необходимо выделять необходимые ресурсы и контролировать состояние дел). Основой программы является *политика безопасности организации* — совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которыми руководствуется организация в своей деятельности. Разработка политики безопасности включает определение следующих основных моментов:

— какие данные и насколько серьезно необходимо защищать;

— кто и какой ущерб может нанести организации в информационном аспекте;

— основные риски и способы их уменьшения до приемлемой величины.

* + практической точки зрения политику безопасности можно условно разделить на три уровня: верхний, средний и нижний.

*К верхнему уровню* относятся решения,затрагивающие организацию в целом(какправило, носят общий характер и исходят от руководства). Например, цели организации в области информационной безопасности, программа работ в области информационной безопасности (с назначением ответственных за ее реализацию).

К *среднему уровню* относятся вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией (например, использование на работе персональных ноутбуков, установка непроверенного программного обеспечения, работа с Интернетом и т.д.).

Политика безопасности *нижнего уровня* касается конкретных сервисов и должна быть наиболее детальной. Часто правила достижения целей политики безопасности нижнего уровня заложены в эти сервисы на уровне реализации [см. 4. С. 148—149].

*Меры процедурного уровня* —отдельные мероприятия,выполняемые на протяжениивсего жизненного цикла АИС. Они ориентированы на людей (а не на технические средства) и подразделяются на:

— управление персоналом;

— физическая защита;

— поддержание работоспособности;

— реагирование на нарушения режима безопасности;

— планирование восстановительных работ.

*Программно-технические меры защиты* основаны на использовании специальныхаппаратных средств и программного обеспечения, входящих в состав АИС и выполняющих функции защиты: шифрование, аутентификацию, разграничение доступа к ресурсам, регистрацию событий, поиск и удаление вирусов и т.д. Они будут подробно рассмотрены в следующих главах.

**Основные принципы построения систем защиты АИС**

* 1. *Простота механизма защиты.* Используемые средства защиты не должны требовать от пользователей специальных знаний или значительных дополнительных трудоза-трат. Они должны быть интуитивно понятны и просты в использовании,.
  2. *Системность.* При разработке системы защиты и вводе ее в эксплуатацию необходим учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для обеспечения безопасности. В частности, должны быть учтены все слабые места АИС, возможные цели и характер атак, возможность появления принципиально новых угроз безопасности.

1. *Комплексность.* Предполагает согласованное применение разнородных средствпри построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Целесообразно строить эшелонированную систему защиты, обеспечивающую комплексную безопасность на разных уровнях (внешний уровень — физические средства, организационные и правовые меры; уровень ОС; прикладной уровень).
2. *Непрерывность.* Мероприятия по обеспечению информационной безопасностиАИС должны осуществляться на протяжении всего ее жизненного цикла — начиная с этапов анализа и проектирования и заканчивая выводом системы из эксплуатации. При этом наилучший результат достигается, когда разработка системы защиты идет параллельно с разработкой самой защищаемой АИС. Не допускается также никаких перерывов в работе средств защиты.
3. *Разумная достаточность.* Один из основополагающих принципов информационной безопасности гласит: абсолютно надежная защита невозможна. Любой самый сложный механизм защиты может быть преодолен злоумышленником при затрате соответствующих средств и времени. *Система защиты считается достаточно надежной,* *если* *средства, которые необходимо затратить злоумышленнику на ее преодоление значительно превышают выгоду, которую он получит в случае успеха.* Иногда используетсяобратный принцип: расходы на систему защиты (включая потребляемые ей системные ресурсы и неудобства, возникающие в связи с ее использованием) не должны превышать стоимость защищаемой информации.
4. *Гибкость.* Система защиты должна иметь возможность адаптироваться к меняющимся внешним условиям и требованиям.

*Открытость алгоритмов и механизмов защиты.* Cистема должна обеспечиватьнадежную защиту в предположении, что противнику известны все детали ее реализации. Или иными словами, защита не должна обеспечиваться за счет секретности структуры и алгоритмов системы защиты АИС.

**Понятие и назначение модели безопасности**

Основную роль в методе формальной разработки системы играет так называемая *модель безопасности* (*модель управления доступом, модель политики безопасности*).Целью этой модели является выражение сути требований по безопасности к данной системе. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации.

Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как она является формальной, возможно осуществить доказательство различных свойств безопасности системы.

Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системе.

Основные понятия, используемые в моделях разграничения доступа, приведены в руководящем документе Государственной технической комиссии при Президенте РФ «Защита от несанкционированного доступа к информации»:

*Доступ к информации* —ознакомление с информацией,ее обработка,в частности,копирование, модификация или уничтожение информации

*Объект доступа* —единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

*Субъект доступа* —лицо или процесс,действия которого регламентируются правилами разграничения доступа.

*Правила разграничения доступа* —совокупность правил,регламентирующих правадоступа субъектов доступа к объектам доступа

**Модель дискреционного доступа (DAC)**

* + рамках дискреционной модели контролируется доступ субъектов (пользователей или приложений) к объектам (представляющим собой различные информационные ресур-сы: файлы, приложения, устройства вывода и т.д.).

Для каждого объекта существует субъект-владелец, который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа. Основными операциями доступа являются READ (чтение), WRITE (запись) и EXECUTE (выполнение, имеет смысл только для программ). Таким образом, в модели дискреционного доступа для каж-дой пары субъект-объект устанавливается набор разрешенных операций доступа.

При запросе доступа к объекту, система ищет субъекта в списке прав доступа объекта и разрешает доступ если субъект присутствует в списке и разрешенный тип доступа включает требуемый тип. Иначе доступ не предоставляется.

Классическая система дискреционного контроля доступа является «закрытой» в том смысле, что изначально объект не доступен никому, и в списке прав доступа описывается набор разрешений. Также существуют «открытые» системы, в которых по умолчанию все имеют полный доступ к объектам, а в списке доступа описывается набор ограничений.

Недостаток модели DAC заключается в том, что субъект, имеющий право на чтение информации может передать ее другим субъектам, которые этого права не имеют, без уведомления владельца объекта. Таким образом, нет гарантии, что информация не станет доступна субъектам, не имеющим к ней доступа. Кроме того, не во всех АИС каждому объекту можно назначить владельца (во многих случаях данные принадлежат не отдель-ным субъектам, а всей системе).

**Модель безопасности Белла—ЛаПадулы**

Одна из наиболее известных моделей безопасности — модель Белла-ЛаПадулы (модель мандатного управления доступом). В ней определено множество понятий, связанных с контролем доступа; даются определения субъекта, объекта и операции доступа, а также математический аппарат для их описания. Эта модель в основном известна двумя основ-ными правилами безопасности: одно относится к чтению, а другое – к записи данных.

Пусть в системе имеются данные (файлы) двух видов: *секретные* и *несекретные,* а пользователи этой системы также относятся к двум категориям: с уровнем допуска к несекретным данным (несекретные) и с уровнем допуска к секретным данным (секретные).

1. *Свойство простой безопасности: несекретный пользователь (или процесс, запущенный от его имени) не может читать данные из секретного файла.*
2. *\*-свойство: пользователь с уровнем доступа к секретным данным не может записывать данные в несекретный файл.* Это правило менее очевидно,но не менее важно.Действительно, если пользователь с уровнем доступа к секретным данным скопирует эти данные в обычный файл (по ошибке или злому умыслу), они станут доступны любому «несекретному» пользователю. Кроме того, в системе могут быть установлены ограничения на операции с секретными файлами (например, запрет копировать эти файлы на дру-гой компьютер, отправлять их по электронной почте и т.д.). Второе правило безопасности гарантирует, что эти файлы (или даже просто содержащиеся в них данные) никогда не станут несекретными и не «обойдут» эти ограничения. Таким образом, вирус, например, не сможет похитить конфиденциальные данные.

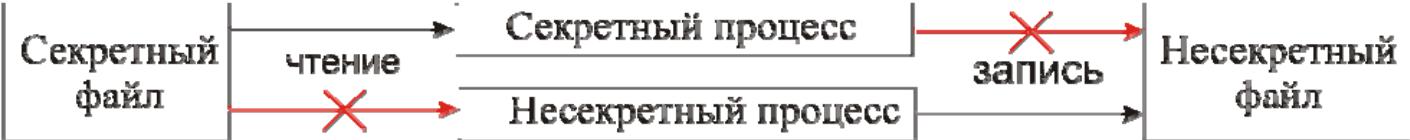


Рис. 2. Модель безопасности Белла-ЛаПадулы.

Рассмотренные правила легко распространить на случай, когда в системе необходимо иметь более двух уровней доступа — например, различаются несекретные, конфиденциальные, секретные и совершенно секретные данные. Тогда пользователь с уровнем допуска к секретным данным может читать несекретные, конфиденциальные и секретные документы, а создавать — только секретные и совершенно секретные.

Общее правило звучит так: *пользователи могут читать только документы,* *уровень* *секретности которых не превышает их допуска, и не могут создавать документы ниже уровня своего допуска.* То есть теоретически пользователи могут создавать документы,прочесть которые они не имеют права.

Модель Белла-ЛаПадулы стала первой значительной моделью политики безопасности, применимой для компьютеров, и до сих пор в измененном виде применяется в военной отрасли. Модель полностью формализована математически. Основной упор в модели делается на конфиденциальность, но кроме неё фактически больше ничего не представлено. Кроме того, в модели игнорируется проблема изменения классификации: предполагается, что все сведения относятся к соответствующему уровню секретности, который оста-ется неизменным. Наконец, бывают случаи, когда пользователи должны работать с данными, которые они не имеют права увидеть. «Сведения о том, что самолет несет груз из некоторого количества бомб, возможно, имеют более высокий уровень секретности, чем уровень доступа диспетчера, но диспетчеру тем не менее необходимо знать вес груза.»

**Ролевая модель контроля доступа (RBAC)**

Ролевой метод управления доступом контролирует доступ пользователей к информации на основе типов их активностей в системе (ролей). Под *ролью* понимается совокупность действий и обязанностей, связанных с определенным видом деятельности. Примеры ролей: администратор базы данных, менеджер, начальник отдела.

В ролевой модели с каждым объектом сопоставлен набор разрешенных операций доступа для каждой роли (а не для каждого пользователя). В свою очередь, каждому пользователю сопоставлены роли, которые он может выполнять. В некоторых системах пользователю разрешается выполнять несколько ролей одновременно, в других есть ограничение на одну или несколько не противоречащих друг другу ролей в каждый момент време-ни.

Для формального определения модели RBAC используются следующие соглашения: *S* =субъект—человек или автоматизированный агент.

*R* =роль—рабочая функция или название,определяется на уровне авторизации. *P* =разрешения—утверждения режима доступа к ресурсу.

*SE* = cессия—Соответствие междуS, Rи/илиP.

*SA* =назначение субъекта(Subject Assignment). *SA* ⊆ *S* × *R*.При этом субъекты назначаются связям ролей и субъектов в отношении «многие ко многим» (один субъект может иметь несколько ролей, а одну роля могут иметь несколько субъектов).

*PA* =назначение разрешения(Permission Assignment). *PA* ⊆ *P* × *R*.При этом разрешения назначаются связям ролей в отношении «многие ко многим».

*RH* =частично упорядоченная иерархия ролей(Role Hierarchy). *PH* ⊆ *R* × *R.*

На возможность наследования разрешений от противоположных ролей накладывается ограничительная норма, которая позволяет достичь надлежащего разделения режимов. Например, одному и тому же лицу может быть не позволено создать учетную запись для кого-то, а затем авторизоваться под этой учетной записью.

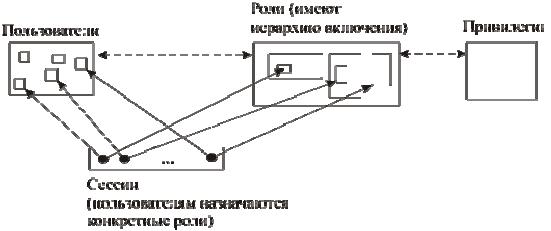


Рис. 3. Схема ролевой модели контроля доступа (RBAC)

Основные достоинства ролевой модели:

1. Простота администрирования. В отличие от модели DAC нет необходимости прописывать разрешения для каждой пары «объект-пользователь». Вместо этого прописываются разрешения для пар «объект-роль» и определяются роли каждого пользователя. При изменении области ответственности пользователя, у него просто изменяются роли. Иерархия ролей (когда роль наряду со своими собственными привилегиями может наследовать привилегии других ролей) также упрощает процесс администрирования.
2. Принцип наименьшей привилегии. Ролевая модель позволяет пользователю регистрироваться в системе ролью, минимально необходимой для выполнения требуемых задач. Запрещение полномочий, не требуемых для выполнения текущей задачи, не позволяет обойти политику безопасности системы.

3. Разделение обязанностей.

RBAC широко используется для управления пользовательскими привилегиями в пределах единой системы или приложения. Список таких систем включает в себя

Microsoft Active Directory, SELinux, FreeBSD, Solaris, СУБД Oracle, PostgreSQL 8.1, SAP R/3 и множество других, эффективно применяющих RBAC.

С помощью RBAC могут быть смоделированы дискреционные и мандатные системы управления доступом.

**Системы разграничения доступа**

Конкретное воплощение модели разграничения доступа находят в *системе разграничения доступа (СРД).* СРД—это совокупность реализуемых правил разграничениядоступа в средствах вычислительной техники или автоматизированных системах.

Многие системы разграничения доступа базируются на *концепции диспетчера доступа.* В основе этой концепции лежит понятие *диспетчера доступа* —абстрактной машины, которая выступает посредником при всех обращениях субъектов к объектам. Диспетчер доступа использует *базу данных защиты*, в которой хранятся правила разграничения доступа и на основании этой информации разрешает, либо не разрешает субъекту доступ к объекту, а также фиксирует информацию о попытке доступа в *системном журнале*.

Основными требованиями к реализации диспетчера доступа являются:

* требование полноты контролируемых операций, согласно которому проверке должны подвергаться все операции всех субъектов над всеми объектами системы. Обход диспетчера предполагается невозможным;
* требование изолированности, то есть защищенности диспетчера от возможных изменений субъектами доступа с целью влияния на процесс его функционирования;
* требование формальной проверки правильности функционирования;
* минимизация используемых диспетчером ресурсов [3].

*База данных защиты* строится на основе матрицы доступа или одного из ее представлений.

Матрица доступа — таблица, в которой строки соответствуют субъектам, столбцы — объектам доступа, а на пересечении строки и столбца содержатся правила (разрешения) доступа субъекта к объекту. Основными недостатками такой матрицы являются ее чрез-мерно большая размерность и сложность администрирования: все взаимосвязи и ограни-чения предметной области приходится учитывать вручную. (Примеры ограничений: права доступа субъекта к файлу не могут превышать его прав доступа к устройству, на котором этот файл размещен; группа пользователей наследует одинаковые полномочия и т.д.). Для преодоления этих сложностей матрица доступа в СРД часто заменяется некоторым ее не-явным *представлением*. Рассмотрим основные из них.

*1. Списки управления доступом* (access control lists, ACL).Для каждого объекта задансписок субъектов, имеющих ненулевые полномочия доступа к ним (с указанием этих полномочий). В результате серьезно экономится память, поскольку из матрицы доступа исключаются все нулевые значения (составляющие большую ее часть). Тем не менее, спискам управления доступом присущ ряд недостатков:

* неудобство отслеживания ограничений и зависимостей по наследованию полномочий субъектов;
* неудобство получения сведений об объектах, к которым имеет какой либо вид доступа данный субъект;
* так как списки управления доступом связаны с объектом, то при удалении субъекта возможно возникновение ситуации, при которой объект может быть доступен несуществующему субъекту.
  1. *Списки полномочий субъектов*. Аналогично ACL с той разницей, что для каждого субъекта задан список объектов, доступ к которым разрешен (с указанием полномочий доступа). Такое представление называется *профилем субъекта*. Оба представления имеют практически идентичные достоинства и недостатки.
  2. *Атрибутные схемы.* Основаны на присвоении субъектам и/или объектам определенных меток, содержащих значения атрибутов. Элементы матрицы доступа не хранятся в явном виде, а динамически вычисляются при каждой попытке доступа для конкретной па-ры субъект-объект на основе их атрибутов. Помимо экономии памяти достигается непротиворечивость базы данных защиты, а также удобство ее администрирования. Основным недостатком является сложность задания прав доступа конкретного субъекта к конкретному объекту.

**Основные понятия криптографии**

До 70-х годов XX века *криптографией* называлась область науки и практической деятельности, связанная с изучением и разработкой методов шифрования данных. В на-стоящее время это область науки, техники и практической деятельности, связанная с раз-работкой, применением и анализом криптографических систем защиты информации.

*Криптографическая система* —это система обеспечения информационной безопасности сети или АИС, использующая криптографические средства. Может включать под-системы шифрования, идентификации пользователей, электронной цифровой подписи и др.

*Криптографические средства* —методы и средства обеспечения информационнойбезопасности, использующие криптографические преобразования информации. В узком смысле под криптографическими средствами могут пониматься отдельные устройства, документы и программы, использующиеся для выполнения функций криптосистемы.

*Криптографическое преобразование информации* —преобразование информации сиспользованием одного из криптографических алгоритмов. К *криптографическим алгоритмам* относятся алгоритмы шифрования/дешифрования,хэширования,формирования ипроверки электронной цифровой подписи, распределения ключей и множество других алгоритмов, каждый из которых предназначен для противодействия определенным угрозам информационной безопасности со стороны возможного нарушителя (противника, злоумышленника) или нежелательных воздействий естественного характера. Большинство криптографических алгоритмов строятся на математической основе.

Криптография является частью боле общей науки — *криптологии*. Вторая часть криптологии — *криптоанализ.* До 70-х годов XX века эта наука занималась оценкой сильных и слабых стором методов шифрования, а также разработкой методов взлома шифров. В настоящее время криптоанализ — область науки, занимающаяся изучением криптографических систем защиты в поиске способов нарушения информационной безопасности, которую обеспечивает данная система. Таким образом, криптоанализ изучает методы прочтения зашифрованного текста без ключа, методы подделки электронной цифровой подписи (без знания закрытого ключа автора) и т.д. Криптография и криптоанализ — две сильно взаимодействующие науки с противоположными целями. За последние не-сколько десятилетий они непрерывно и интенсивно развиваются, причем достижения одной из них заставляют другую быстро реагировать совершенствованием своего аппарата.

**Шифрование**

Шифрование — это процесс преобразования исходного сообщения M (называемого *открытым текстом*)в формуM' (*зашифрованный текст* или *шифртекст*).При этомпровести обратное преобразование M' в M возможно только обладая некоторой дополни-тельной информацией, называемой *ключом*.

Шифрование нередко путают с *кодированием*, но между двумя этими процессами есть значительная разница. Кодирование также представляет собой преобразование исходного сообщения в другую форму, но цель этого преобразования — удобство обработки или передачи сообщения. Например, символьный текст кодируется в двоичный (каждый символ заменяется последовательностью нулей и единиц) для того, чтобы его можно было хранить и обрабатывать в ЭВМ, а двоичный текст преобразовывается в последовательность электрических импульсов, для того, чтобы стала возможной его передача по кабелю. Цель шифрования — противоположная. Текст зашифровывается для того, чтобы посторонние лица, не обладающие ключом, не могли бы воспринять заложенную в нем ин-формацию, даже располагая этим зашифрованным текстом. Таким образом, шифрование является *средством обеспечения конфиденциальности* информации.

Алгоритмы шифрования делятся на две большие группы:

1. Симметричное (традиционнное шифрование).
2. Шифрование с открытым ключом.

**Симметричное шифрование**

* + - симметричных алгоритмах шифрования *один и тот же ключ* K используется для того, чтобы зашифровать сообщение и для его последующей расшифровки. Таким обра-зом, и *отправитель* и *получатель* сообщения должны располагать одним и тем же клю-чом. Схематично это можно записать в виде:

M' = E(M, K) M = D(M', K),

где Е — функция шифрования (encrypt), а D — функция дешифрования (decrypt), обе используют ключ K в качестве одного из параметров.

Исторически симметричное шифрование появилось первым. Более того, до середины XX века это была единственная разновидность шифрования. Симметричные алгоритмы широко применяются и в настоящее время.

Далее мы рассмотрим ряд простых алгоритмов симметричного шифрования, на при-мере которых легко проанализировать такие их характеристики, как устойчивость к раз-личным видам криптоанализа, а также некоторые базовые принципы криптографии. Затем будут рассмотрены алгоритмы, используемые в современных информационных системах.

Все алгоритмы симметричного шифрования можно разделить на три класса:

* 1. Подстановочные алгоритмы.
  2. Перестановочные алгоритмы.
  3. Алгоритмы, использующие и подстановку и перестановку (к этому классу относят-ся практически все современные алгоритмы, разработанные для защиты информации в ЭВМ).

***Подстановочные алгоритмы***

Подстановочные алгоритмы шифрования работают по следующему принципу:

*каждый символ (или последовательность символов) исходного сообщения заменяются другим символом (или другой последовательностью символов).*

Рассмотрим конкретные примеры.

**1. Шифр Цезаря.**

Самым древним и самым простым из известных подстановочных шифров является шифр, использовавшийся Юлием Цезарем. В этом шифре каждая буква исходного сообщения заменяется буквой, находящейся в алфавите на три позиции после нее.



Рис. 1. Пример шифрования по Цезарю

Особенностью шифра Цезаря, как несложно заметить, является отсутствие ключа. Часло 3 в данном случае ключом не является, поскольку не выбирается отправителем со-общения, а используется для сдвига по алфавиту постоянно. Во времена Юлия Цезаря это не было слабостью шифра (поскольку сама идея сокрытия информации путем преобразования текста была незнакомой его противникам), но в настоящее время первым правилом криптографии является следующее допущение:

*Стойкость любого шифра определяется в предположении, что противнику полностью известен механизм шифрования и единственной информацией, которой он не рас-полагает, является ключ.*

Данное допущение особенно актуально для настоящего времени, когда сложность шифров достигла такого уровня, что зашифровывать и расшифровывать сообщения вручную просто невозможно. Для этих целей используется программное обеспечение, которое заинтересованные лица могут детально проанализировать и, таким образом, полностью восстановить алгоритм шифрования.

Это правило имеет тенденцию нарушаться в тех областях, когда криптографиечское программное обеспечение не предназначено для широкого распространения. Например, алгоритмы, использующиеся в системах электронного голосования, правительственной связи и др. Разработчики этих систем считают сокрытие алгоритмов шифрования факто-ром, усиливающим безопасность. Однако считается научно установленной ошибочность этого предположения. Злоумышленник, серьено заинтересованный в том, чтобы взломать криптографическую защиту и нарушить конфиденциальность данных, почти наверняка найдет способ получить доступ к самой программе, которая по определению не может быть также хорошо защищена, как обрабатываемые ею данные, и изучить используемые алгоритмы. Сокрытие алгоритмов и деталей архитектуры таких систем лишь препятствует их изучению независимыми исследователями и увеличивает опасность того, что алгоритмы, положенные в их основу, будут недостаточно надежными.

Рассмотрим вариацию шифра Цезаря, при которой число 3 является не жестко заданным, а выбирается произвольно, согласно договоренности между отправителем и получателем сообщения. В этом случае шифр Цезаря становится полноценным шифром с ключом K (потенциально неизвестном противнику).

Однако легко заметить, что в качестве ключа могут быть выбраны лишь числа в диапазоне от 1 до 32 (для русского алфавита). Действительно, шифр является циклическим: Я + 1 = А, но и Я + 34 = А. То есть, число 34, выбранное в качестве ключа, будет эквивалентно ключу 1, ключ 35 — ключу 2 и т.д. Противнику ничего не стоит перебрать все 32 возможных ключа и обнаружить нужный[4](file:///F:\1%20курс\Методичка\__77037(1).docx#page29).

Таким образом, модифицированный шифр Цезаря является неустойчивым ко взлому методом перебора возможных ключей по причине их малого диапазона или, как говорят,

малой длины ключа.

**Моноалфавитный шифр (шифр простой замены)**

Один из хорошо известных подстановочных шифров. Каждому символу алфавита открытого текста ставится в соответствие некоторый символ другого алфавита. Он может и совпадать с первым (тогда одна буква заменяется другую). При шифровании каждая символ открытого текста заменяется на соответствующий ему другой символ.

Ключом к данному шифру будет являться таблица соответствий, которую удобно представить в виде символов, выписанных в алфавитном порядке тех букв, которые они заменяют. Другими словами, ключом является перестановка символов алфавита зашифрованного текста.

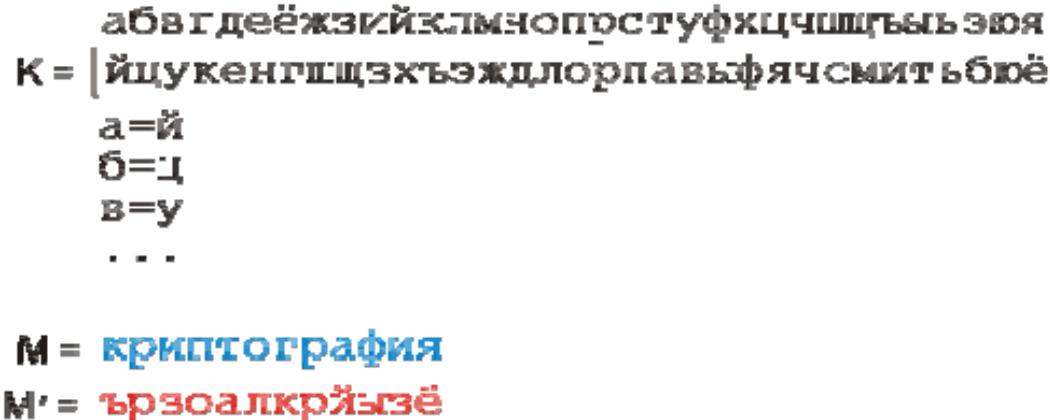


Рис. 2. Пример шифрования текста шифром простой замены

В данном случае число возможных ключей равно числу возможных перестановок из 33 букв, то есть, 33!. Даже при использовании миллиона компьютеров, проверяющих миллион возможных ключей в секунду, перебор всех вариантов займет больше миллиона лет. Таким образом, моноалфавитный шифр является стойким ко взлому методом перебора возможных ключей.

Однако данный шифр достаточно просто поддается криптоанализу, который начинается с подсчета каждого символа шифртекста и определения частоты его встречаемости.

Для достаточно длинного сообщения (порядка 4—5 предложений) этой информации будет достаточно, чтобы сопоставить ее с таблицей частоты встречамости букв языка.

Все естественные языки имеют характерное частотное распределение символов. На-пример, буква «О» - встречается в русском языке чаще других, а буква «Ф» — самая ред-кая (см. табл. 1).

*Табл. 1. Таблица частот встречаемости букв русского языка.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Символ | Вероятность | Символ | Вероятность | Символ | Вероятность |
|  |  |  |  |  |  |
| пробел | 0.175 | К | 0.028 | Ч | 0.012 |
|  |  |  |  |  |  |
| О | 0.089 | М | 0.026 | Й | 0.010 |
|  |  |  |  |  |  |
| Е | 0.072 | Д | 0.025 | Х | 0.009 |
|  |  |  |  |  |  |
| А | 0.062 | П | 0.023 | Ж | 0.007 |
|  |  |  |  |  |  |
| И | 0.062 | У | 0.021 | Ю | 0.006 |
|  |  |  |  |  |  |
| Н | 0.053 | Я | 0.018 | Ш | 0.006 |
|  |  |  |  |  |  |
| Т | 0.053 | Ы | 0.016 | Ц | 0.004 |
|  |  |  |  |  |  |
| С | 0.045 | З | 0.016 | Щ | 0.003 |
|  |  |  |  |  |  |
| Р | 0.040 | Ь | 0.014 | Э | 0.003 |
|  |  |  |  |  |  |
| В | 0.038 | Б | 0.014 | Ф | 0.002 |
|  |  |  |  |  |  |
| Л | 0.03 | Г | 0.013 |  |  |
|  |  |  |  |  |  |

На основе частоты встречаемости символов зашифрованного текста можно сделать предположения о некоторых, наиболее часто встречающихся из них, а затем, опираясь на эти предположения, постепенно восстанавливать слова текста, начиная с самых коротких

— предлогов и союзов. Так, в английском языке достаточно легко идентифицируется артикль the — самая часто встречающаяся комбинация из трех букв.

Таким образом, моноалфавитные шифры имеют серьезную слабость к криптоанализу на основе статистических особенностей исходного текста, которые наследует зашифрованный текст. Противнику даже не нужно целенаправленно подбирать ключ — он сам восстанавливается по ходу дела.

Нетрудно заметить, что шифр Цезаря также является моноалфавитным шифром.

**Современные алгоритмы симметричного шифрования**

Современные алгоритмы симметричного шифрования используют как подстановку, так и перестановку. Стандартом де-факто являются несколько раундов шифрования с разными ключами, которые генерируются на основе одного общего ключа. Большинство современных алгоритмов имеют структуру, аналогичную структуре шифра Файстеля, разработанного в 1973 году.

Шифр Файстеля создавался как пример практической реализации идеи Клода Шеннона: надежный алгоритм шифрования должен удовлетворять двум свойствам: диффузии и коффузии.

Диффузия — каждый бит открытого текста должен влиять на каждый бит зашифрованного текста. Суть диффузии заключается в рассеянии статистических характеристик открытого текста внутри шифрованного текста.

Конфузия — отсутствие статистической взаимосвязи между ключом и зашифрованным текстом. Даже если противник определит какие-то статистические особенности за-шифрованного текста, их должно оказаться недостаточно, чтобы получить любую информацию о ключе.

Рассмотрим структуру шифра Файстеля.

Данный шифр относится к категории блочных. Блочные шифры предназначены для шифрования небольших блоков определенной длины. Для того, чтобы зашифровать произвольный текст, его необходимо разбить на блоки, после чего каждый блок зашифровывается отдельно (вариации рассматриваются в следующем разделе). Кроме того, как и практически все современные алгоритмы, шифр Файстеля работает с двоичным алфавитом (т.е. и открытый и зашифрованный текст представлены последовательностью битов) и предназначен для реализации на ЭВМ.

На вход алгоритма шифрования подается блок открытого текста, имеющий четную длину 2l и ключ K. Блок разделяется на две равные части — правую R0 и левую L0. Далее эти части проходят m раундов обработки, после чего снова объединяются в зашифрованный текст.

Каждый i-й раунд состоит в генерации подключа Ki (на основе общего ключа K) и применении к блоку Ri некоторого зависящего от ключа преобразования F. Результат складывается с блоком Li с помощью операции XOR (исключающее или) и получается блок Ri+1. Блок Ri без изменений берется в качестве блока Li+1.

Процесс дешифрования принципиально ничем не отличается, но на вход подается зашифрованный текст, а ключи Ki вычисляются в обратном порядке.

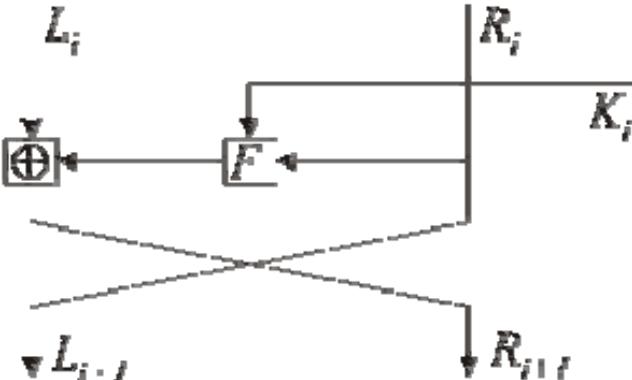


Рис. 8. Схема i-го раунда шифрования шифра Файстеля

Различные алгоритмы, использующие структуру шифра Файстеля могут отличться следующими параметрами:

1. Длина ключа. Чем длиннее ключ, предусмотренный алгоритмом, тем сложнее осуществить перебор. Сейчас надежной считается длина ключа не менее 1024 бита.

2. Размер блока. Чем выше размер блока, тем больше надежность шифра, но скорость операций шифрования/дешифрования при этом снижается.

3. Число раундов обработки. С каждым новым раундом обработки надежность шифра повышается.

4. Функция раунда F — чем она сложнее, тем труднее криптоанализ шифра.

5. Алгоритм вычисления промежуточных ключей Ki.

**Алгоритм DES**

Долгое время самым популярным алгоритмом симметричного шифрования являлся DES (Data Encrypting Standart), принятый в 1977 году. Этот алгоритм базируется на структуре шифра Файстеля с размером блока 64 бита и 56-битным ключом.

Функция раунда F использует набор из восьми так называемых S-матриц. Каждая матрица состоит из 4 строк, причем каждая строка представляет собой перестановку чисел от 0 до 15 (соответственно, 16 столбцов). Матрицы жестко заданы8. Каждая матрица по 8 S-матрицы считались самой сомнительной частью алгоритма DES, поскольку создатели алгоритма не раскрыли принципы их заполнения — почему выбраны именно эти матрицы и не содержит ли алгоритм

Получает на вход шесть бит и выдает четырехбитовый результат. Первый и последний бит входного значения задают строку матрицы, а четыре остальных — столбец. Двоично представление числа, находящегося на их пересечении, и будет результатом преобразования. Собственно же преобразование F заключается в следующем:

1. 32-битовый блок Ri расширяется до 48 битов с помощью специальной таблицы пу-тем дублирования некоторых 16 битов.

2. Полученный результат складывается с 48-битным подключом Ki операцией XOR.

3. Результат сложения разбивается на 8 шестибитовых блоков и каждый из них пре-образуется с помощью соответствующей S-матрицы.

4. Получившийся в итоге 32-битный блок подвергается жестко заданной в алгоритме перестановке.

Долгое время DES являлся федеральным стандартом шифрования США. Этот алгоритм показывает хороший лавинный эффект (изменение одного бита открытого текста или ключа приводит к изменению многих битов зашифрованного текста) и успешно противостоял многолетним попыткам взлома. Однако длина ключа в 56 битов при возросшей производительности ЭВМ сделала шифр потенциально уязвимым к перебору ключей, по-этому в 1997 году был объявлен конкурс на новый алгоритм, который должен был стать криптостандартом на ближайшие 10-20 лет.

**Алгоритм AES**

Победитель конкурса был определен в 2000 году — им стал бельгийский шифр

RIJNDAEL, который был переименован в AES (Advanced Encryption Standard). Он является нетрадиционным блочным шифром, поскольку не использует сеть Фейштеля. Каждый блок входных данных представляется в виде двумерного массива байт ( 4х4, 4х6 или 4х8 в зависимости от размера блока, которая может варьироваться). В зависимости от размера блока и длины ключа алгоритм содержит от 10 до 14 раундов, в каждом из которых про-водится ряд преобразований — либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами в таблице.

Среди других современных алгоритмов симметричного шифрования следует назвать шифры IDEA, Blowfish, RC5, CAST-128.

**Режимы функционирования блочных шифров**

Симметричные алгоритмы шифрования можно разделить на две категории: блочные и потоковые. В потоковых алгоритмах символы (байты или биты) исходного текста шифруются последовательно. Классическим примером является одноразовый блокнот или шифр простой замены. В блочных шифрах единицей шифрования является блок (последовательность бит фиксированной длины), который преобразуется в блок зашифрованного текста такой же длины. Как отмечалось выше, большинство современных симметричных алгоритмов шифрования относятся к категории блочных шифров.

«тайных ходов». Однако за годы попыток взлома этого алгоритма слабости S-матриц так и не были выявлены.

Существует четыре основных режима работы блочных шифров, которые предназначены для их оптимального применения в самых различных областях.

1. Режим электронной шифровальной книги (ECB). Наиболее простой и естественный способ. Текст разбивается на блоки и каждый блок шифруется с одним и тем же ключом. Основной недостаток подхода заключается в том, что одинаковые блоки будут одинаково зашифровано, что снижает защиту в случае больших объемов шифруемой информации.

2. Режим сцепления шифрованных блоков (CBC). Каждый блок открытого текста перед шифрованием объединяется с помощью операции XOR с предыдущим блоком зашифрованного текста. Первый блок объединяется с некоторым заранее заданным инициализационным вектором. В результате одинаковые блоки открытого текста в зашифрованном виде будут различаться.

3. Режим шифрованной обратной связи (CFB). Похож на предыдущий, но основное назначение состоит в том, чтобы превратить блочный шифр (например, DES с дли-ной блока 64 бита) в потоковый, т.е. шифрующий по одному символу (размером, например, j = 8 бит). Идея заключается в том, что изначально 64-битовый буфер заполняется значением инициализационного вектора (известного отправителю и получателю), которое шифруется ключом K. Из полученного результата выбираются старшие (левые) j бит, которые объединяются с помощью XOR с первым символом открытого текста. Получаем первый зашифрованный символ. Далее содержимое буфера сдвигается на j бит влево, а в самый младшие (правые) j бит записывается зашифрованный символ. Система готова к шифрованию следующего символа.

4. Режим обратной связи по выходу (OFB). Аналогичен предыдущему, но в младшие j бит буфера после сдвига помещается не зашифрованный символ, а j сташих бит результата шифрования (т.е. до их объединения с символом открытого текста). Та-кой режим более устойчив к помехам (сбой при передаче одного символа зашифрованного текста не будет влиять на результаты дешифрования других символов).

**Скремблеры**

Одним из распространенных потоковых алгоритмов шифрования является скремб-лер. Скремблерами называются программные или аппаратные реализации алгоритма, по-зволяющего шифровать побитно непрерывные потоки информации. Сам скремблер пред-ставляет из себя набор бит, изменяющихся на каждом шаге по определенному алгоритму. После выполнения каждого очередного шага на его выходе появляется шифрующий бит – либо 0, либо 1, который накладывается на текущий бит информационного потока опера-цией XOR.

Рассмотрим пример простого скремблера. Он задается двумя битовыми последовательностями равной длины, одна из которых называется ключом (начальной последовательностью), а вторая собственно скремблером (часто вторая последовательность является фиксированной для конкретной аппаратной или программной реализации, а ключ выбирается как в обычном симметричном шифровании). Чем больше длина ключа (и скремблера), тем более надежным будет алгоритм.

Начальная последовательность (ключ) накладывается на скремблер, представляю-щий собой маску: выбираются только те биты последовательности, позициям которых со-ответствует единица в скремблере. Далее выбранные биты складываются между собой операцией XOR. Получается новый бит, который записывается в начало (слева) ключа. Последний (правый) бит ключа становится первым символом кодирующей последовательности и отбрасывается. Таким образом, происходит сдвиг ключа и генерация одного бита. Этот бит накладывается на первый бит исходного текста операцией XOR и получается первый бит зашифрованного текста. После этого цикл повторяется.

Пусть необходимо зашифровать сообщение 00111 скремблером 101 с ключом 011. Вычисляется сумма по модулю 2 первого и третьего бита ключа: 1 ⊕ 1 = 0. Этот бит становится новым первым битом ключа, а последний бит ключа (1) становится битом шифрующей последовательности. Вычисляем первый бит зашифрованного текста: 1 ⊕ 0 = 1. Далее повторям процесс, но уже с ключом 101. Шифрование всего сообщения показано на рисунке.



Рис. 9. Скремблирование последовательности 00111 скремблером 101 с ключом 011

**Основные разновидности криптоанализа симметричных шифров**

Классическая задача криптоанализа — получение открытого текста по зашифрован-ному тексту, не располагая при этом ключом. Часто под этим подразумевается нахождение ключа.

Некоторые методы криптоанализа шифров обсуждались выше при рассмотрении со-ответствующих алгоритмов шифрования.

Одна из популярных классификаций методов криптоанализа — по тем данным, которыми должен располагать аналитик. Соответственно выделяют:

— Анализ только шифрованного текста. Криптоаналитику известны алгоритм шифро-вания и зашифрованный текст.

— Анализ с известным открытым текстом. Криптоаналитик дополнительно располагает несколькими парами соответствующих друг другу фрагментов открытого и зашифрованного текста, созданного с одним и тем же ключом.

— Анализ с избранным открытым текстом. Криптоаналитик имеет возможность выби-рать открытый текст для шифрования (т.е. располагает интересующим его открытым текстом и соответствующим ему зашифрованным).

— Анализ с избранным зашифрованным текстом. Криптоаналитик имеет возможность выбирать получать открытый текст для некоторых интересующих его образцов откры-того текста.

— Анализ с избранным текстом. Возможности криптоаналитика включают два предыдущих случая.

Существуют также отдельные методы криптоанализа, широко применяющиеся для взлома современных шифров. Перечислим наиболее известные из них.

Статистический криптоанализ. Основан на подсчете частоты встречаемости от-дельных символов (или групп символов) в зашифрованном тексте. Подходит для взлома симметричных подстановочных алгоритмов.

Дифференциальный криптоанализ. Разновидность анализа с избранным открытым текстом. Используется при взломе современных симметричных алгоритмов шифрования, в которых текст последовательно проходит несколько раундов преобразований (в частно-сти, известен алгоритм дифференциального криптоанализа шифра DES). Метод основан на прослеживании изменения схожести между двумя текстами. Выбирается пара неза-шифрованных текстов с определенным отличием (X), после чего анализируются отличия, получившиеся после шифрования одним раундом алгоритма, и определяются вероятности различных ключей. Если для многих пар входных значений, имеющих одно и то же отличие Х, при использовании одного и того же подключа одинаковыми (Y) оказываются и отличия соответствующих выходных значений, то можно говорить, что Х влечет Y с оп-ределенной вероятностью. Эта вероятность и присваивается данному подключу раунда. Затем выбирается подключ с наибольшей вероятностью. Процесс повторяется для всех раундов. Цель — определить таким образом все подключи данного ключа (сам ключ при этом может остаться неизвестным).

Линейный криптоанализ. Применяется для взлома блочных симметричных шифров. В основе лежит понятие линейного приближения — предположение о том, что если вы-полнить выполнить операцию XOR над некоторыми битами открытого текста, затем над некоторыми битами шифротекста, а затем над результатами, получится бит, который представляет собой XOR некоторых бит ключа. Если это предположение верно с вероятностью выше ½, то на основе большого числа известных пар открытый текст/зашифрованный текст можно с удовлетворительной вероятностью определить значения отдельных битов ключа.

**Проблемы симметричных алгоритмов**

Все алгоритмы симметричного щифрования имеют общую проблему, проистекаю-щую из того обстоятельства, что и отправитель и получатель сообщения должны обладать одним и тем же ключом. При этом предполагается, что у них нет абсолютно надежного канала связи, поскольку в противном случае в шифровании бы не было нужды.

Если столетие назад эта проблема вполне решалась, например, путем личной встречи. Но в настоящее время, когда интенсивность обмена информацией возросла в сотни раз и автоматизированы практически все сферы человеческой деятельности, это невозможно. Необходимость в срочной конфиденциальной переписке может возникнуть у деловых партнеров, живущих в разных странах (и, может быть, даже не знакомых лично). Интерет-банкинг позволяет управлять своим банковским счетом, не выходя из дома, но при этом все операции должны быть конфиденциальными, а следовательно, весь поток данных между банком и клиентом должен быть зашифрован. При этом ключи шифрования должны регулярно меняться, поскольку обмен даже несколькими сообщениями с одним ключом уменьшает надежность шифрования.

Таким образом, для симметричных алгоритмов характерна проблема обмена ключа-ми. В настоящее время существует несколько способов ее решения, которые будут рассматриваться далее.

Кроме того, возникает проблема управления большим количеством ключей, по-скольку отдельный ключ необходим для каждой пары «отправитель-получатель». Если группа из n человек желает обмениваться конфиденциальными сообщениями, понадобит-ся O(n2) ключей (n-1 ключ каждому). Если же группа будет использовать один общий ключ, то его компрометация (утечка) у одного члена скомпрометирует переписку всей группы.

Эти проблемы и привели к появлению в середине XX века приницпиально нового класса алгоритмов шифрования.

**Алгоритмы шифрования с открытым ключом**

В алгоритмах шифрования с открытым ключом каждый пользователь имеет пару ключей, связанных друг с другом некоторой зависимостью. Ключи обладают свойством:

* текст, зашифрованный одним ключом, может быть расшифрован только с помощью парного ему ключа. Один ключ называется секретным (закрытым) ключом. Пользователь хранит свой секретный ключ в надежном месте и никому его не передает. Второй ключ называется открытым ключом, и пользователь, напротив, сообщает его всем желающим (а также может опубликовать в любом общедоступном источнике).

Если пользователь A хочет отправить зашифрованное послание пользователю B, он шифрует его с помощью открытого ключа B. Теперь текст не сможет прочесть никто, кроме B (даже сам A), поскольку для дешифрования нужен закрытый ключ.

Схему шифрования можно записать в следующем виде:

M' = E(M, Kоткр)

M = D(M', Kзакр),

где Е — функция шифрования (encrypt), D — функция дешифрования (decrypt), а Kоткр и Kзакр — соответственно открытый и закрытый ключи получателя сообщения.

Принципиальный метод шифрования с открытым ключом впервые был публично предложен в 1976 году Диффи и Хеллманом. При этом они не смогли придумать конкретного алгоритма, но сформулировали принципиальные условия, которым такие алгоритмы должны удовлетворять:

1. Процесс генерации пары ключей (открытый и закрытый) не должен представлять вычислительных трудностей.

2. Процесс зашифрования текста, т.е. вычисления E(M, Kоткр), а также процесс де-шифрования, т.е. вычисления D(M', Kзакр) также не должны представлять вычислительных трудностей.

3. Для противника должно быть невозможно (с точки зрения вычислительных возможностей) вычисление закрытого ключа Kзакр по имеющемуся открытому ключу Kоткр.

4. Для противника должно быть невозможно (с точки зрения вычислительных воз-можностей) вычисление открытого текста M по имеющемуся зашифрованному тексту M' и открытому ключу Kоткр.

Кроме этого желательно, чтобы операции шифрования и дешифрования выполня-лись в любом поряке, т.е. можно было бы зашифровать текст закрытым ключом, а рас-шифровать открытым. Преимущества этой возможности будут рассмотрены позже.

**Алгоритм RSA**

RSA — один из первых алгоритмов шифрования с открытым ключом — разработан в 1977 году, название составлено из первых букв имен его авторов (Райвест, Шамир и Ад-леман). На протяжении двадцати лет он был самым опулярным и практически единствен-ным широко использующимся алгоритмом с открытым ключом.

Рассмотрим этот алгоритм подробно.

По теореме Эйлера Mϕ(n)

Для генерации ключей выбираются два больших случайных простых числа p и q и вычисляется их произведение n = pq. Затем вычисляется функция Эйлера: ϕ(n) = (p-1)(q-1)

Далее выбирается целое число e, такое что 1 < e < ϕ(n) и e взаимно просто с ϕ(n). Находится число d такое, что ed ≡ 1 (mod ϕ(n)). Это может быть сделано, например, при помощи расширенного алгоритма Евклида.

Открытым ключом является пара чисел (n, e), а закрытым ключом — пара (n, d). Как видно, для того, чтобы по открытому ключу определить закрытый, необходимо вычислить ϕ(n), а для этого большое (на практике порядка 1024 битов) число n необходи-мо разложить на простые множители. Но эффективного алгоритма разложения числа на простые множители не существует.

RSA предназначен для шифрования двоичных текстов. Открытый текст разбивается на блоки и каждый блок рассматривается как двоичное число M. При этом должно соблю-даться ограничение M < n, исходя из этого условия выбираются длина блока и минималь-но возможные значения p и q.

Для того, чтобы зашифровать сообщение, вычисляется

M' = Me mod n

Для дешифрования необходимо вычислить

M= M'd mod n

Убедимся в корректности алгоритма.

M'd mod n = (Me mod n)d mod n = Med mod n

Т.к. ed ≡ 1 (mod ϕ(n)), то ed ≡ kϕ(n) + 1 для некоторого целого k. Отсюда:

Med mod n = Mkϕ(n) + 1 mod n

≡ 1 (mod n). Т.о.:

Mkϕ(n) + 1 mod n = M

Получили M'd mod n = M, что и требовалось доказать.

Очевидно, что открытый и закрытый ключ в алгоритме RSA взаимозаменяемы: то, что зашифровано одним из них, расшифровывается другим.

Недостатком алгоритмов с открытым ключом является низкая скорость выполняемых операций. Так, в алгоритме RSA шифрование и дешифрование заключается в возве-дении очень большого числа в очень большую степень, а это достаточно ресурсоемкая операция.

Поэтому на практике чаще всего используется комбинация двух алгоритмов. Сообщение шифруется с помощью симметричного алгоритма шифрования (например, AES). При этом каждый раз генерируется новый случайный ключ. Этот ключ зашифровывается открытым ключом получателя (например, с помощью RSA) и отправляется вместе с со-общением. Такая гибридная схема обеспечивает как скорость операций шифрова-ния/дешифрования, так и надежность.

**Электронная цифровая подпись**

Как отмечалось выше, многие алгоритмы шифрования с открытым ключом работают со взаимозаменяемой парой ключей, т.е. любым из них можно зашифровать текст и тогда расшировываться он будет вторым ключом.

Для целей конфиденциальности текст шифруется открытым ключом получателя. Рассмотрим ситуацию, когда сообщение шифруется закрытым ключом отправителя.

В этом случае расшифровать его сможет кто угодно, поскольку открытый ключ общедос-тупен. Однако получатель сообщения может быть уверен в том, что подлинный автор со-общения — владелец закрытого ключа, поскольку никто другой не имеет возможности его создать (при условии, что закрытый ключ не скомпрометирован, т.е. не украден). Таким образом, достигается аутентичность (подлинность) сообщения. С юридической точки зрения это означает, что автор сообщения не сможет от него отказаться (апеллируемость).

Эта идея нашла свое воплощение в концепции электронной цифровой подписи. Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в ре-зультате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сер-тификата ключа подписи, а также установить отсутствие искажения информации в элек-тронном документе. Такое определение приводится в ст. 3 федерального закона «Об элек-тронной цифровой подписи».

В качестве электронной цифровой подписи может выступать сам текст сообщения, зашифрованный закрытым ключом отправителя. Однако такой вариант не используется в силу его неэффективности. Во-первых, шифрование/дешифрование всего текста занимает очень много времени. Во-вторых, длина ЭЦП в этом случае будет равна (и даже превы-шать) длину исходного сообщения, что создает неудобство при пересылке. Поэтому со-временные алгоритмы электронной цифровой подписи основаны на использовании хэш-функций.

Хэш-функцией называется функция (H), которая принимает на входе сообщение M произвольной длины, а на выходе выдает значение H(M) фиксированной длины, называе-мое хэшем или профилем сообщения М. При этом в криптографии (в частности, в алго-ритмах ЭЦП) используются функции, обладающие следующими свойствами:

1. Односторонность. Для любого хэша h должно быть практически невозможно вы-числить или подобрать такое x, что H(x) = h.

2. Стойкость к коллизиям первого рода. Для любого сообщения x должно быть прак-тически невозможно вычислить или подобрать другое сообщение y, такое что H(x) = H(y).

3. Стойкость к коллизиям второго рода. Должно быть практически невозможно вы-числить или подобрать любую пару различных сообщений x и y для которых H(x) = H(y).

Среди наиболее известных алгоритмов хэширования можно назвать MD5, SHA-512, ГОСТ Р34.11 (российский стандарт вычисления хэш-функции).

**Роль парольной защиты в обеспечении безопасности АИС**

Криптографические методы, в частности, шифрование, хорошо обеспечивают защи-ту информации (конфиденциальности, целостности, аутентичности и т.д.) от внешнего нарушителя. Такой нарушитель, возможно, может перехватывать сообщения, передаю-щиеся по каналу связи а, в некоторых случаях, модифицировать их и даже вставлять в се-анс связи собственные сообщения (зачастую стараясь выдать их за сообщения другого источника). Однако информация в канале связи предварительно подвергается криптографическим преобразованиям и передается в соответствии с криптографическими протокола-ми, специально разработанными для того, чтобы помешать нарушителю реализовать угро-зы безопасности. Для того, чтобы нарушить безопасность информации, циркулирующей в системе, ему необходимо найти уязвимость в системе защиты, либо в использованных в ней криптографических алгоритмах. Аналогичные трудности встают перед нарушителем, получившим доступ к защищенной АИС в качестве пользователя, не обладающего привилегиями, необходимыми для доступа к интересующим его данным.

Однако ситуация меняется, если нарушитель получает доступ в систему от имени пользователя, уполномоченного выполнять операции с интересующими его данными (на-пример, копирование конфиденциальных файлов, уничтожение критически важных данных и т.д.). В этом случае вся криптографическая защита оказывается бесполезной. Таким образом — самое уязвимое место автоматизированной информационной системы — точки доступа к ней. Эти точки доступа защищаются протоколами аутентификации (проверки подлинности пользователя). А самая удобная для пользователя и наиболее используемая форма аутентификации — парольная защита.

Поэтому в большинстве случаев злоумышленника, который тем или иным образом может добраться до точки входа в систему (с рабочего места пользователя или удаленным способом), от его цели отделяет только пароль — вводимый с клавиатуры набор симво-лов. Часто пароль выбирается неопытными пользователями таким образом, что его легко подобрать, в отличие от случайных 1024-битных криптографических ключей)13; часто не принимаются должные организационные меры по обеспечению безопасности пароля.

Существует ряд стандартных приемов, применяемых злоумышленниками с целью обойти парольную защиту. Для каждого из этих приемов выработан механизм противо-действия. На основе этих механизмов можно сформулировать правила выбора безопасно-го пароля и работы с ним.

**Способы атаки на пароль. Обеспечение безопасности пароля**

Рассмотрим приемы обхода парольной защиты и методы противодействия им.

**1. Полный перебор (метод грубой силы, bruteforce).**

Самая простая (с технической точки зрения) атака на пароль — перебор всех комби-наций допустимых символов (начиная от односимвольных паролей). Современные вычислительные мощности позволяют перебрать все пароли длиной до пяти-шести символов за несколько секунд.

Некоторые системы не позволяют реализовать атаки, основанные на переборе, поскольку реагируют на несколько попыток неправильно набранного пароля подряд. На-пример, ОС Windows после трех неудачных попыток входа в систему делает минутную паузу (что делает полный перебор практически нереализуемым), а сим-карты сотовых те-лефонов и кредитные карточки банкоматов полностью блокируются.

Однако существует множество систем, позволяющих бесконечный перебор. Напри-мер, к защищенному паролем файлу (архив rar или zip, документ Microsoft Office и т.д.) можно пробовать разные пароли бесконечно. Существует множество программ, которые позволяют автоматизировать эту процедуру: Advanced RAR Password Recovery, Advanced PDF Password Recovery, Advanced Office XP Password Recovery. Кроме того, многие про-

граммы хранят хэш пароля в доступном файле. Например, таким образом клиент для ра-боты с электронной почтой (работающий на общедоступном компьютере) может хранить пароли пользователей. Существуют способы похитить файл, содержащий хэши паролей доступа к операционной системе. После этого можно заниматься подбором паролей уже в обход системы, с помощью специальных программ.

Важной характеристикой пароля, затрудняющей (и даже делающей невозможным) полный перебор, является его длина. Современный пароль должен иметь длину не менее 12 символов.

Два лишних символа в пароле (при условии, что в нем могут встречаться все символы, которые можно набрать с клавиатуры, т.е. порядка 200) увеличивают время перебора в 40000 раз, а четыре символа — уже в 1.600.000.000 раз. Для того, чтобы перебрать все возможные пароли длиной 15 символов, потребуется время большее, чем возраст Вселен-ной. Однако не стоит забывать, что вычислительные мощности компьютеров постоянно растут (еще несколько лет назад безопасным считался пароль длиной 8 символов).

**2. Перебор в ограниченном диапазоне.**

Известно, что многие пользователи, составляя пароль, используют символы, находящиеся в определенном диапазоне. Например, пароль, состоящий только из русских букв или только из латинских букв или только из цифр. Такой пароль значительно легче за-помнить, однако задача противника, осуществляющего перебор, неимоверно упрощается.

Пусть n = 70 — количество символов, из которых можно составить пароль, причем 10 из них — цифры, 30 — буквы одного языка и 30 — буквы другого языка. Пусть мы составляем пароль длиной m = 4 символа.

Если пароль составляется абсолютно случайно, то количество возможных комбинаций (которые необходимо перебрать) составляет 704 = 24010000. Однако противник может сделать предположение, что пароль состоит из символов одного диапазона (пусть даже, неизвестно, какого). Всего таких паролей 104 + 304 + 304 = 10000 + 810000 + 810000 = 163000. Если он оказался прав, то количество комбинаций (а следовательно, время, кото-рое необходимо затратить на перебор) уменьшилось в 147 раз. Это число резко возрастает, когда увеличивается длина пароля и число диапазонов символов, из которых он может быть составлен.

Программы автоматического перебора пароля (такие как Advanced Office XP Password Recovery) включают опцию, позволяющую перечислить символы, которые сле-дует пробовать при подборе пароля.

Как следствие, надежный пароль должен содержать в себе символы из различных диапазонов. Рекомендуется использовать русские и английские, прописные и строчные буквы, цифры, а также прочие символы (знаки препинания, подчеркивание и т.д.).

**3. Атака по словарю**

Бессмысленный, абсолютно случайный пароль труден для запоминания. Между тем угроза забыть пароль и потерять важную информацию для многих пользователей выглядит гораздо реальнее и страшнее, чем взлом их системы неизвестным злоумышленником. Поэтому в качестве пароля очень часто выбирается какое-то слово.

В этом случае задача подбора пароля превращается для злоумышленника почти в тривиальную Программа автоматического перебора паролей проверяет слова, содержа-щиеся в заданном файле со словарем (существует огромное количество доступных слова-рей такого рода для разных языков). Словарь из двухсот тысяч слов проверяется такой программой за несколько секунд.

Многие пользователи считают, что если применить к задуманному слову некоторое простое преобразование, например, написать его задом наперед или русскими буквами в английской раскладке или намеренно сделать ошибку, то это обеспечит безопасность. На самом деле, по сравнению с подбором случайного пароля подбор пароля по словарю с применением различных преобразований (сделать первую букву заглавной, сделать все буквы заглавными, объединить два слова и т.д.) делает невыполнимую задачу вполне возможной.

Надежный пароль не должен строиться на основе слов естестенного языка.

**4. Атака по персональному словарю**

Если атака по словарю и перебор паролей небольшой длины либо составленных из символов одной группы не помогает, злоумышленник может воспользоваться тем фактом, что для облегчения запоминания, многие пользователи выбирают в качестве пароля личные данные (номер сотового телефона, дату рождения, записанную наоборот, кличку со-баки и т.д.).

В том случае, если цель злоумышленника — обойти парольную защиту именно этого пользователя, он может составить для него персональный словарь личных данных, по-сле чего использовать программу автоматического перебора паролей, которая будет генерировать пароли на основе этого словаря.

Таким образом, надежный пароль должен быть полностью бессмысленным.

**5. Сбор паролей, хранящихся в общедоступных местах**

Во многих организациях пароли создает и распределяет системный администратор, который использует приведенные выше правила. Пользователи обязаны пользоваться вы-данным им паролем. Однако, поскольку этот пароль сложно запомнить, он часто хранится под рукой в записанном виде. Нередки случаи, когда пароль записывается на стикер и приклеивается к монитору, либо содержатся в записной книжке, которая часто лежит на столе раскрытой.

Проблема в том, что, как показывают исследования, пользователи зачастую несерьезно относятся к вопросам обеспечения безопасности своего служебного пароля. Обычно это происходит из за непонимания политики безопасности организации и недооценки важности тех данных или сервисов, которые защищены паролем. Кроме того, пользователи считают, что, поскольку в организации «все свои», небрежное хранения пароля вреда не наносит. Между тем, проникнуть в помещение организации под благовидным предло-гом и провести визуальный осмотр — достаточно простая задача для злоумышленника.

Более того, часто получив пароль от администратора на бумажке и переписав его в записную книжку, пользователи теряют или просто выбрасывают эту бумажку. В поисках пароля злоумышленики иногда не брезгуют копаться и в мусоре.

Пароль не должен храниться в общедостпуном месте. Идеальный вариант — запомнить его и не хранить нигде. Если пароль содержится в записной книжке, она не должна оставляться без присмотра, а при вводе пароля не должно присутствовать посторонних, которые могут заглянуть в книжку через плечо.

**6. Социальный инжиниринг**— манипулирование людьми (а не машинами) с целью проникновения в защищенные системы пользователя или организации. Если подобрать или украсть пароль не удается, можно попытаться обманом заставить пользователя отдать пароль самому. Классическая тактика социального инжиниринга — телефонный звонок жертве от имени того, кто имеет право знать запрашиваемую информацию. Например, злоумышленник может представиться системным администратором и попросить сообщить пароль (или другие сведения) под убедительным предлогом. Склонение пользовате-ля к открытию ссылки или вложения, которые открывать не следует (см. главу 4) или заманивание его на подставной сайт (см. следующий пункт) также относят к методам социального инжиниринга.

Приемы, используемые злоумышленником, могут быть самыми разными. Начиная от звонка среди ночи с абсолютно неправдоподобной историей типа «в нашу банковскую сеть попал вирус и он уничтожает все данные о счетах клиентов, а мы не можем их спасти, потому что вирус уничтожил файл с паролями — срочно скажите ваш и мы спасем ваши деньги».

В любом случае, необходимо помнить правило: сообщать пароль посторонним ли-цам ни в коем случае нельзя. Даже если эти лица имеют право его знать14. Единственным исключением может являться требование суда или правоохранительных органов выдать пароль под угрозой ответственности за отказ от дачи показаний. Но и в этом случае необходимо убедиться, что сотрудники правоохранительных органов — именно те, за кого они себя выдают.

7. **Фишинг** — это процедура «выуживания» паролей случайных пользователей Интернета. Обычно заключается в создании «подставных» сайтов, которые обманом вынуждают пользователя ввести свой пароль.

Например, чтобы получить пароль к банковскому счету, может быть создан сайт с дизайном, идентичным сайту некоторого банка. Адрес этого сайта, естественно, будет другим, но чаще всего злоумышленник регистрирует доменное имя, отличающееся от банковского на один символ. В результате пользователь, сделав опечатку, попадет на под-ставной сайт и не заметит своей ошибки. Для заманивания пользователей клиентам банка могут также рассыласться электронные письма с содержанием типа «проверьте свой счет» или «ознакомьтесь с новыми акциями», причем в письме содержится ссылка, ведущая на подставной сайт.

Когда клиенты банка попадают на сайт злоумышленника, им (как и на настоящем сайте) предлагается ввести логин и пароль для доступа к счету. Эта информация сохраняется в базе данных злоумышленника, после чего клиент перенаправляется на главную страницу настоящего сайта. Пользователь видит, что ввод пароля «не сработал» и думает, что совершил ошибку или сайт просто «глючит». Он пробует ввести пароль заново и на этот раз успешно входит в систему. Это рассеивает его подозрения. Между тем, утечка пароля уже произошла...

Другая разновидность фишинга основана на том факте, что многие пользователи ис-пользуют один и тот же пароль для разных ресурсов. В результате, произведя успешную атаку на менее защищенный ресурс, можно получить доступ к более защищенному.

Например, создается сайт, потенциально интересный некоторому кругу пользовате-лей. Если цель атаки — конкретный человек, то предварительно изучаются его интересы и увлечения. Информация об этом сайте доносится до потенциальных жертв (персонально или за счет широкой рекламы). Пользователю, зашедшему на сайт, предлагается зарегистрироваться, в частности, придумать себе пароль. Теперь остается только посмотреть, не подходит ли введенный пароль к другим ресурсам этого пользователя (например, к электронной почте, адрес которой был указан при регистрации).

Чтобы противостоять угрозе фишинга необходимо внимательно проверять адрес сайта, прежде чем вводить важный пароль. Лучше всего поместить этот адрес в закладки браузера и пользоваться исключительно этими закладками, ни в коем случае не переходя по ссылкам из электронных писем. Наконец, следует пользоваться разными паролями для доступа к разным сервисам.

**Компьютерные вирусы и борьба с ними**

**Общие сведения о компьютерных вирусах**

Компьютерным вирусом называется программа, способная к саморазмножению.

Это означает, что программа, будучи запущенной, способна создавать свои копии (возможно, модифицированные) и распространять их некоторым образом с компьютера на компьютер. При этом, как правило, внедрение вируса на компьютер и его запуск происходит без ведома (и вопреки желанию) владельца компьютера.

Вирус, как программа, состоит из двух частей: механизм размножения и начинка. Механизм размножения определяет способ, которым копии вируса создаются, распространяются и запускаются. Начинка представляет собой дополнительное поведение вируса (помимо размножения) на зараженном компьютере.

Начинка некоторых вирусов является вполне безобидной (например, вывод сообщения на экране), а некоторых — весьма опасной: уничтожение данных, похищение информации или использование компьютера в качестве плацдарма для DdOS-атаки. В любом случае вирус оказывает негативное воздействие, расходуя ресурсы процессора, оперативную память и дисковое пространство. Кроме того, масштабная эпидемия вируса, размножающегося по сети, когда оказываются зараженными тысячи компьютеров, может привести к тому, что сеть выйдет из строя из-за перегрузки. По этой причине вирусы называют вредоносными программами.

Вообще под вредоносной программой (malware) эксперты понимают любую программу, которая устанавливает себя на компьютер без ведома его владельца и осуществляет нежелательные для него функции.

Другое определение вредоносного программного обеспечения (которое, в частности, взято на вооружение российскими правоохранительными органами) — это любое ПО, написанное с целью нанесения ущерба или использования ресурсов атакуемого компьютера.

**Классификация вирусов**

По начинке вирусы делятся на деструктивные и недеструктивные. Деструктивные вирусы классифицируют по выполняемым ими функциям:

1. Вирусы, уничтожающие данные. Наиболее характерный пример — вирус «Чернобыль» (Win95.CIH), массовое распространение которого случилось в 1999 году. При запуске проверял системную дату компьютера и 26 апреля активировал механизм уничтожения данных на жестком диске16. Другой вирус, Klez.E, произвел эпидемию в 2002 году. Он срабатывал на шестой день каждого нечетного месяца и заполнял файлы определенных форматов (.doc, .txt и др.) случайным содержимым, после чего их восстановление становилось невозможным.

2. Вирусы-шпионы. Начинка заключается в похищении информации, например, отслеживании всех нажатий пользователя на клавиатуру, записи этих данных в специальный файл и регулярной отправки создателю вируса. Другой вариант — пересылка файлов с паролями и учетных данных платежных систем.

3. Использование зараженных компьютеров в качестве плацдарма для рассылки спама или распределенной DоS-атаки (группа зараженных таким вирусом компьютеров называется «зомби-сетью»). Пример такого вируса — MsBlast — был предназначен для атаки на сайт windowsupdate.com: 16 августа 2003 года со всех зараженных компьютеров осуществлялись запросы к этому сайту, в результате чего сервер должен был подвергнуться критической перегрузке и выйти из строя.

4. Крипто-вирусы. Шифруют информацию на жестком диске алгоритмом с открытым ключом и предлагают пользователю (например, оставив текстовый файл с сообщением) купить закрытый ключ, переведя деньги на определенный счет.

Общепринятая классификация вирусов — по механизму их размножения. Выделяются файловые вирусы, макровирусы, загрузочные вирусы и сетевые черви. Рассмотрим все эти разновидности более подробно.

**Файловые вирусы**

Файловые вирусы внедряются в исполняемые файлы на компьютере (заражают их), дописывая самих себя в начало, в середину или в конец файла. Таким образом, при запуске пользователем зараженного файла автоматически будут выполнены и команды вируса (поиск незараженных файлов, их заражение, а также начинка).

Распространение таких вирусов происходит через зараженные файлы. Достаточно принести один такой файл на незараженный компьютер и запустить его, чтобы вирус на-чал действовать. Спустя короткое время все исполняемые файлы на компьютере оказываются зараженными и при запуске любой программы вместе с ней срабатывает и вирус.

Файловые вирусы были весьма распространены в 90-х годах, когда программы были небольшими и распространялись «из рук в руки» на дискетах. В настоящее время эти ви-русы непопулярны, не в последнюю очередь потому, что их достаточно легко обнаружить: во-первых, увеличивается размер всех исполняемых файлов, а во-вторых, многие про-граммы при запуске проверяют свою целостность (например, по размеру или контрольной

сумме) и сигнализируют о ее нарушении. Тем не менее, опасность скачать из Интернета или по пиринговой сети зараженный файл по-прежнему остается.

**Макровирусы**

Макровирусы не отличаются по механизму размножения от файловых вирусов; их особенность в том, что заражают они не исполняемые файлы, а файлы некоторых популярных форматов документов (в частности, .doc и .xls). Макровирусы оказались опасны тем, что пользователи привыкли к мысли о том, что зараженной может быть только программа и не опасались получить вирус вместе с документом.

Макровирусы используют возможности некоторых программ (текстовых, графических, табличных редакторов, СУБД и пр.) внедрять в документы, создаваемые этими программами, так называемые макросы — процедуры, написанные на встроенном в них языке программирования и выполняемые в ответ на определенные события (нажатие пользователем кнопки или открытие документа). Например, Microsoft Office поддерживает встроенный язык программирования Visual Basic for Applications (VBA).

Макровирус представляет собой программу на макроязыке, внедренную в документ соответствующего формата и запускающуюся автоматически обычно при открытии документа. После запуска вирус ищет другие доступные документы этого формата и внедряется в них, а также исполняет свою начинку (возможностей современных макроязыков вполне хватает, чтобы эта начинка могла содержать серьезные деструктивные функции).

В настоящее время макровирусы также непопулярны, поскольку современные версии программ, поддерживающих макроязыки, предупреждают пользователя о наличии макросов в документе. Более того, чтобы позволить макросу запуститься, от пользователя нередко требуется изменить настройки программы.

**Сетевые черви**

Современные вирусы не заинтересованы в том, чтобы заразить как можно больше файлов на компьютере (и тем самым повысить вероятность своего запуска и размножения). С повсеместным проникновением Интернета наиболее привлекательная цель для вирусов — проникнуть на как можно большее число компьютеров в сети. При этом достаточно, чтобы на каждом компьютере содержался лишь один экземпляр вируса, но при этом соблюдалось два условия:

1. Вирус должен автоматически запускаться (желательно одновременно с запуском операционной системы).

2. Содержащий вирус файл должен быть надежно скрыт от пользователя.

Вирусы, которые автоматически запускаются в момент старта операционной системы и, таким образом, постоянно функционируют в оперативной памяти, называются резидентными. Вирусы, распространяющие свои копии по локальной сети или через Интернет называются сетевыми червями. Большинство сетевых червей являются резидентными.

Вирусы, распространяющиеся через Интернет, являются наиболее популярными и представляют наибольшую угрозу. Они имеют два основных механизма проникновения на компьютер жертвы:

1. Через стандартные коммуникационные сервисы.

2. Через «дыры» в популярных сетевых приложениях, в том числе самой ОС.

В роли стандартного коммуникационного сервиса чаще всего выступает обыкновенная электронная почта. Вирус распространяется в виде прикрепленного к электронному письму файлового вложения, которое доверчивые и халатные пользователи, имеющие низкую культуру в области информационной безопасности, из любопытства запускают, отдавая тем самым свой компьютер под контроль вируса.

Этому способствует тот факт, что письмо с вирусным вложением может прийти со знакомого почтового адреса. Действительно, заразив компьютер, почтовый вирус, как правило, обрабатывает файл, в котором содержится адресная книга почтовой программы, и извлекает из нее адреса постоянных корреспондентов пользователя, после чего им направляются автоматически сгенерированные письма с копией вируса.

Один из самых нашумевших сетевый червей — вирус «I love you», эпидемия которого началась 4 мая 2000 года. После открытия файла, приложенного к электронному письму, вирус уничтожал или изменял некоторые файлы на зараженной машине, а кроме того сразу же, в момент запуска, рассылал себя по всем адресам адресной книги пользователя. По оценкам различных компаний, поражению подверглось огромное количество компьютерных сетей (в отдельных странах — от 30 до 80 процентов). Количество получателей «любовных писем» оценивается в 45 миллионов человек, общие убытки — до 10 миллиардов долларов США17. Адресат получал письмо следующего содержания:

Subject «ILOVEYOU»

Сообщение: «kindly check the attached LOVELETTER coming from me.» Присоединенный файл: «LOVE-LETTER-FOR-YOU.TXT.vbs»

Несмотря на то, что механизм проникновения вирусов через почтовые вложения имеет достаточно почтенный возраст и широко известен, пользователи по-прежнему заражаются почтовыми вирусами, неосторожно запуская вложения.

Второй механизм заражения — ошибки в сетевых программах, позволяющие вредоносной программе проникать на компьютер пользователя и получать на нем управление без каких-либо действий со стороны самого пользователя. Такие вирусы появляются значительно реже (поскольку обнаружение подобной ошибки и написание программы, кото-рая ей пользуется, непросто). Однако, появившись, они вызывают серьезную вирусную эпидемию (как вирус MsBlast в 2003 году), которая прекращается только тогда, когда вы-пускается патч (программа, исправляющая уязвимость) и его устанавливают большинство пользователей.

Единственный способ хоть как-то противостоять подобным вирусам — своевременная установка обновлений.

Рассмотрим теперь резидентные вирусы. Их характерной особенностью является автоматический запуск после загрузки операционной системы. Большинство резидентных вирусов под Windows обеспечивает выполнение этого условия, прописывая себя в разде-лы автозагрузки в реестре:

HKEY\_LOCAL\_MACINE\Software\Microsoft\Windows\CurrentVersion\Run HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\

При этом многие вирусы, резидентно находясь в памяти, следят за реестром и если пользователь удаляет соответствующую запись (ключ), восстанавливают ее. Поэтому чтобы удалить вирус вручную, необходимо загрузиться в безопасном режиме.

Маскируются сетевые черви в большинстве своем в системных папках Windows (например, System32) среди сотен файлов, назначение которых пользователю неизвестно.

**Загрузочные вирусы**

Загрузочные вирусы заражают носители данных. Изначально заражению подвергались дискеты и жесткие диски. Загрузочный вирус прописывает себя в первый (нулевой) сектор раздела, где обычно находится программа-загрузчик. Сама эта программа перемещается в другое место, а при загрузке с зараженного носителя сначала запускается вирус. Вирус предпринимает меры к тому, чтобы закрепиться в оперативной памяти и получить контроль над системой, после чего позволяет загружаться стандартному загрузчику.

Классические загрузочные вирусы в настоящее время устарели, поскольку загрузка с дискеты (а именно на дискетах такие вирусы и распространялись) уже практически не используется. Однако в последние годы появилась вариация вирусов (которые также можно назвать загрузочными), распространяющиеся через флэш-накопители.

Такой вирус представляет собой обычный исполняемый файл с атрибутом «скрытый», который записывается в корневой каталог флешки либо в скрытую папку, эмулирующую корзину Windows либо другую системную папку. Кроме этого в корневом рата-логе размещается файл autorun.inf со ссылкой на вирус. Вирус активируется, если у флешки срабытывает автозапуск, а это обычно происходит автоматически, если открывать флешку двойным щелчком по ее ярлыку при условии, что настройки Windows установлены по умолчанию. Вирус оставляет свои копии (вместе с autorun.inf) на всех разделах жесткого диска и, таким образом, получает управление во время каждого сеанса работы пользователя, когда тот случайно активирует автозапуск на одном из этих разделов. Далее вирус постоянно находится в оперативной памяти, исполняет свою начинку, а также отслеживает подключение к компьютеру новых переносных носителей и заражает их.

Для профилактики таких вирусов (помимо антивирусной защиты) необходимо открывать переносные устройства таким образом, чтобы не позволить сработать автозапуску. Например, открывать их через оболочку типа Total Commander, либо через адресную строку проводника Windows (но не двойным щелчком по ярлыку).

**Троянские кони**

Троянским конем (разг.: троян, троянец) называется вредоносная программа, которая не имеет (в отличие от вирусов) способности к саморазмножению, а вместо этого маскируется под программу, выполняющую полезные функции. Таким образом, распространение троянских коней часто происходит посредством самих пользователей, которые скачивают их из Интернета или друг у друга, не догадываясь о последствиях.

Особая опасность в том, что пользователи принимают их за легальные программы. Поэтому запуская троянского коня пользователь может вручную (в ответ на предупреждение операционной системы или файервола) дать ей все необходимые права, открыть доступ в Интернет и к системным ресурсам.

Одна из распространенных начинок троянских коней — бэкдор (backdoor) — программа, позволяющая злоумышленнику получать удаленный доступ к системе (а в некоторых случаях полностью ее контролировать).

**Технологии маскировки вирусов**

Помимо начинки и механизма размножения интерес представляют приемы, с помощью которых вирусы скрывают свое присутствие в системе, с тем, чтобы продержаться в ней как можно дольше.

Стелс-вирус — вирус, полностью или частично скрывающий свое присутствие путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т.д.) Например, файловый вирус может перехватывать функции чтения/записи в файл, чтения каталога и т. д., чтобы скрыть увеличение размера зараженных программ; перехватывает функции чтения/записи файла в память, чтобы скрыть факт изменения файла.

Полиморфные вирусы — вирусы, модифицирующие свой код в зараженных про-граммах таким образом, что два экземпляра одного и того же вируса могут не совладать ни в одном бите. Это затрудняет анализ и обнаружение его антивирусом. Для модификации кода используется шифрование. Т.е. вирус содержит шифратор, причем при размножении каждая копия вируса шифруется новым случайным ключом, а расшифровывает вирус сам себя уже во время выполнения. Естественно, дешифратор при этом не зашифровывается, но полиморфные вирусы обычно содержат код генерации дешифратора, чтобы, выполняя одни и те же функции, эта часть в каждой копии вируса имела различный вид.

**Тенденции современных компьютерных вирусов**

Рассмотрим характерные черты, которые за последние годы наиболее четко проявились в современных вирусах:

— наибольшее распространение получили сетевые черви;

— вирусы активно используют уязвимости в различных операционных системах и программном обеспечении;

— для быстрого распространения вирусов используются спам-технологии;

— один вирус сочетает в себе множество технологий: полиморфных, стелс, бэкдор;

— вместо пересылки своего тела по электронной почте часто отправляется ссылка на веб-сайт или на зараженный ранее компьютер;

— увеличивается число вирусов для новых платформ: КПК, сотовых телефонов, смартфонов и коммуникаторов, при этом активно используются беспроводные среды передачи данных (Bluetooth, Wi-Fi).

**Борьба с вирусами**

Для борьбы с вирусами используется специальное программное обеспечение — антивирусы. По выполняемым ими функциям выделяют следующие виды антивирусов:

— Программы-детекторы осуществляют поиск характерного для вируса кода (сигнатуры) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение.

— Программы-доктора или фаги также осуществляют поиск зараженных файлов и «лечат» их, т.е. возвращают в исходное состояние. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

— Ревизоры запоминают исходное состояние объектов незараженной системы и периодически сравнивают текущее состояние с исходным.

— Программы-фильтры — резидентные (то есть постоянно работающие) программы, предназначенные для обнаружения при работе компьютера подозрительных действий, характерных для вирусов.

— Вакцины — резидентные программы, предотвращающие заражение файлов. Современные антивирусы представляют собой многофункциональные программные

комплексы, которые способны обнаруживать, лечить (удалять) вирусы, а также препятствовать их проникновению на компьютер.

Современные антивирусы могут работать в двух режимах. В режиме монитора антивирус постоянно работает, отслеживая все обращения системы к файлам, вклиниваясь в этот процесс и проверяя эти файлы на предмет заражения. Таким образом, при первой попытке вируса активироваться антивирус блокирует эту попытку и выдает предупреждение. При использовании режима монитора работа компьютера замедляется (так как часть вычислительных ресурсов тратится на работу антивируса, а любое ображение к файлам и некоторым другим объектам сопровождается процедурой сканирования). Кроме того, если на компьютере присутствуют зараженные файлы, которые не проявляют активности и об-ращения к ним не происходит, они останутся незамеченными.

В режиме сканера антивирус проверяет все файлы в заданной области (определен-ный каталог, раздел жесткого диска или все устройства хранения информации) и удаля-ет/лечит зараженные (либо просто оповещает о них — в зависимости от настроек скане-ра). Проверка всех данных на компьютере может занять значительное время (несколько часов). Кроме того, вирус может попасть в систему сразу после сканирования.

Для надежной защиты рекомендуется применение обоих режимов: постоянная работа антивируса в режиме монитора и регулярная (раз в неделю) проверка всех данных с помощью сканера (обычно сканирование запускается на ночь).

Рассмотрим методы обнаружения антивирусом своих жертв.

Обнаружение, основанное на сигнатурах — метод работы антивирусов и систем обнаружения вторжений, при котором антивирус, просматривая файл (или передаваемый по сети пакет), обращается к словарю, в котором содержатся сигнатуры известных атак или вирусов. Под сигнатурой понимается фрагмент кода, однозначно идентифицирующий вирус. Например, вирус Email-Worm.Win32.Happy содержит строку «Happy New Year 1999 !!», которая с низкой вероятностью может встретиться в другой программе.

Основной принцип, по которому выделяются сигнатуры — она должна содержать только уникальные строки из этого файла, настолько характерные, чтобы гарантировать минимальную возможность ложного срабатывания. Разработка сигнатур осуществляется вручную путем кропотливого исследования нескольких файлов, зараженных (или принадлежащих) одним вирусом. Автоматическая генерация сигнатур (особенно в условиях полиморфных вирусов) пока не дает удовлетворительных результатов.

Каждый современный антивирус имеет обширную (несколько сот тысяч) базу сигна-тур, которая регулярно обновляется. Проблема обнаружения, основанного на сигнатурах заключается в том, что новый вирус (сигнатуры которого еще нет в базе) может беспрепятственно обойти антивирусную защиту. При этом создание сигнатуры и доставка ее пользователям занимает от 11 до 97 часов в зависимости от производителя, в то время как теоретически, вирус может захватить весь интернет меньше, чем за 30 секунд18.

Метод обнаружения подозрительного поведения программы. Антивирус прослеживает поведение всех работающих программ и пытается выявить действия, характерные для вируса (например, запись данных в exe-файл). Однако этот метод часто вызывает ложные срабатывания (в результате пользователи перестают обращать внимание на предупреждения). Разновидность этого метода — эмуляция программы: перед запуском при-ложения антивирус пытается имитировать его поведение с целью отслеживая подозри-тельных действий. Данный метод наиболее требователен к ресурсам.

Метод «белого списка». Предотвращается выполнение всех компьютерных кодов кроме тех, которые были ранее обозначены системным администратором как безопасные.

Эвристическое сканирование — метод, основанный на сигнатурах и эвристике, при-зван улучшить способность сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда сигнатура совпадает с телом неизвестной про-граммы не на 100 %, но в подозрительной программе налицо более общие признаки виру-са. Данная технология, однако, применяется в современных программах очень осторожно, так как может повысить количество ложных срабатываний19.

Наиболее известные современные антивирусы: антивирус Касперского, Doctor WEB, NOD32, Norton Antivirus, Panda Antivirus, Avast! Antivirus (последний является бесплатным для домашнего использования).

**Средства защиты сети**

Если локальная сеть организации или персональный компьютер пользователя имеют выход в сеть Интернет, количество угроз безопасности увеличивается в десятки раз по сравнению с изолированной сетью или компьютером. Сетевые вирусы, попытки проник-новения в систему извне (используя подобранный или украденный пароль, уязвимости программного обеспечения и т.д.), перехват и подмена данных, передаваемых в сеть или получаемых из сети — вот перечень наиболее типичных угроз.

Существует ряд средств, методов и технологий защиты информации, учитывающих специфику сетевых атак. К ним, в частности, относятся межсетевые экраны (брандмауэры), виртуальные частные сети (VPN) и системы обнаружения вторжений.

**Межсетевые экраны**

Межсетевой экран (брандмауэр, файрвол) — комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него се-тевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Межсетевой экран, как правило, обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким об-разом трафик передается из одной сети в другую. Если в правиле отсутствует явное раз-решение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты.

Межсетевой экран может выступать в роли proxy-сервера. Proxy-сервер — это про-грамма или узел сети, играющий роль посредника между внутренней сетью организации и внешней сетью (например, Интернет). В этом случае он может также скрывать внутренние адреса компьютеров организации. Эта функция называется трансляцией сетевых адресов (NAT — Network Address Translation). Когда какой-то узел внутренней сети хочет переда-вать информацию вовне, он отправляет ее proxy-серверу (одновременно являющемуся межсетевым экраном). Проверив передаваемые пакеты на соответствие политике фильт-рации, межсетевой экран инициирует новое соединение, и передает пакеты уже от своего имени. В результате скрывается схема внутренней адресации сети и тем самым сущест-венно затрудняется ее анализ злоумышленником (с целью обнаружения уязвимостей).

Существует ряд классификаций межсетевых экранов по различным критериям:

**1. В зависимости от охвата контролируемых потоков данных.**

— Традиционный межсетевой экран — программа, установленная на шлюзе (сервере пе-редающем трафик между сетями) или аппаратное решение, контролирующие входя-щие и исходящие потоки данных между подключенными сетями. Основная задача та-кого брандмауэра — предотвращение несанкционированного доступа во внутреннюю сеть организации.

— Персональный межсетевой экран — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

**2. В зависимости от уровня модели OSI, на котором происходит контроль доступа.**

— Работающие на сетевом уровне — фильтрация происходит на основе адресов отпра-вителя и получателя пакетов, номеров портов транспортного уровня модели OSI и ста-тических правил, заданных администратором;

— Работающие на сеансовом уровне — отслеживаются сеансы между приложениями и не пропускаются пакеты, нарушающие спецификации TCP/IP (такие пакеты часто ис-пользуются в злонамеренных операциях: сканировании ресурсов, взломах через не-правильные реализации TCP/IP, обрыв/замедление соединений и т.д.).

— Работающие на уровне приложений — фильтрация на основании анализа данных при-ложения, передаваемых внутри пакета; передача потенциально опасной и нежелатель-ной информации блокируется на основании политик и настроек.

**3. В зависимости от отслеживания активных соединений.**

— Stateless (простая фильтрация) — не отслеживают текущие соединения (например, TCP), а фильтруют поток данных исключительно на основе статических правил;

— Stateful (фильтрация с учётом контекста) — отслеживают текущие соединения и пропускают только такие пакеты, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений.

Рассмотрим некоторые популярные брандмауэры, реализованные в виде прикладных программ.

1. Outpost Firewall Pro. Персональный брандмауэер, обладает следующими функциональными возможностями:

— предотвращение несанкционированного доступа к данным;

— сокрытие присутствия зщищаемой системы в сети (таким образом она делается «неви-димой» для взломщиков);

— анализ входящих почтовых сообщений и блокировка потенциально опасных;

— мониторинг и анализ сетевой активности системы;

— блокировка доступа к «запрещенным» сайтам (для детей или сотрудников).

2. ZoneAlarm Pro. Мощный брандмауэр с гибко настраиваемыми функциональными возможностями, включающими:

— фильтр приложений, позволяющий устанавливать права для каждой программы, ис-пользуемой в сети;

— поддержку цифровой подписи;

— подробный лог-файл событий и средства для его анализа, с последующей выдачей тек-стовых и графических отчетов;

— настраиваемый контроль cookies;

— механизм мгновенной автоматической или ручной блокировки доступа приложений к Интернет;

— автоматическую проверку вложений электронной почты.

**Виртуальные частные сети (VPN)**

Виртуальная частная сеть (VPN) — логическая сеть, создаваемая поверх другой сети, чаще всего Интернет. Все данные, передающиеся между узлами этой сети шифруются, поэтому, хотя физически данные передаются по публичным сетям с использованием не-

безопасных протоколов, по сути, VPN представляет собой закрытые от посторонних каналы обмена информацией.

Канал между двумя узлами, защищенный за счет шифрования проходящего по нему трафика, называется туннелем.

Выделяют два основных класса VPN:

1. Защищенные. Наиболее распространённый вариант. C его помощью на основе ненадёжной сети (как правило, Интернета) создается надежная и защищенная подсеть. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP (протокол тунеллирования от точки к точке).

2. Доверительные. Используются для создания виртуальной подсети в рамках другой, надежной и защищенной сети, т.е. задача обеспечения безопасности по сути не ставится. К доверительным VPN относятся протоколы MPLS и L2TP.

По архитектуре технического решения выделяют следующие классы VPN:

1. Внутрикорпоративные. Предназначены для обеспечения защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными связями, включая выделенные линии.

2. VPN с удаленным доступом. Предназначены для обеспечения защищенного удаленного доступа мобильных или удаленных сотрудников компаний к корпоративным информационным ресурсам.

3. Межкорпоративные (extranet VPN). Обеспечивают прямой защищенный доступ из сети одной компании к сети другой компании (партнера, клиента и т.д.).

По способу технической реализации различают VPN на основе маршрутизаторов (задача шифрования трафика ложится на маршрутизаторы, через которые проходит вся исходящая из локальных сетей информация), на основе межсетевых экранов, на основе программного обеспечения и на основе специализированных аппаратных средств.

Рассмотрим набор протоколов IPSec, предназначенный для обеспечения защиты данных, передаваемых по протоколу IP. Он позволяет осуществлять подтверждение подлинности и шифрование IP-пакетов, а также включает протоколы для защищенного обмена ключами через Интернет.

Протоколы IPsec работают на сетевом уровне модели OSI. Они подразделяются на два класса: протоколы отвечающие за защиту потока передаваемых пакетов (ESP, AH) и протоколы обмена ключами (IKE). Протоколы защиты передаваемого потока могут работать в двух режимах — в транспортном режиме и в режиме туннелирования. В транспортном режиме шифруется (или подписывается) только информативная часть IP-пакета, а заголовок не затрагивается (поэтому процедура маршрутизации не изменяется). В туннельном режиме IP-пакет шифруется целиком. Для того, чтобы его можно было передать по сети, он помещается в другой IP-пакет. Именно этот режим используется для организации виртуальной частной сети.

Режим IPSec-тунеллирования работает следующим образом [6]:

1. Обычный IP-пакет посылается на отправляющее IPSec-устройство (межсетевой экран или маршрутизатор), где он должен быть зашифрован и направлен в конечную систему по локальной сети.

2. Отправляющее IPSec-устройство проводит аутентификацию принимающего устройства.

3. Два IPSec-устройства «договариваются» о шифре и алгоритме аутентификации, которыми будут пользоваться.

4. Отправляющее IPSec-устройство шифрует IP-пакет с информацией и помещает его в другой пакет с AH (аутентифицирующим заголовком).

5. Пакет пересылается по сети (по протоколам TCP/IP).

6. Принимающее IPSec-устройство читает IP-пакет, проверяет его подлинность и извлекает зашифрованное вложение для расшифровки.

7. Принимающее устройство отправляет исходный пакет в пункт его назначения.

**Системы обнаружения вторжений (IDS)**

Система обнаружения вторжений (Intrusion Detection System — IDS) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими (в основном через Интернет).

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которые могут нарушить безопасность системы или сети. К ним относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (вирусов, троянских коней).

Структурно СОВ состоит из следующих компонентов:

1. Сенсорная подсистема отслеживает события, которые могут затрагивать безопасность защищаемой системы.

2. Подсистема анализа выявляет среди этих событий те, которые представляют уг-розу или нарушения безопасности (атаки, подозрительные действия). В пассивных СОВ при обнаружении такого события информация о нем помещается в хранилище, после чего сигнал опаности по определенному каналу направляется администратору системы. Активные СОВ (системы предотвращения вторжений) могут также предпринять ответные действия (например, прервать соединение или автоматически настроить межсетевой экран для блокирования трафика от злоумышленника).

3. Хранилище обеспечивает накопление и хранение данных сенсорной подсистемы и результатов их анализа;

4. Консоль управления используется для настройки СОВ, наблюдения за состоянием защищаемой системы, просмотра выявленных подсистемой анализа инцидентов.

Рассмотрим основные разновидности современных СОВ [8].

1. СОВ, защищающие сегмент сети. Развертываются на специализированном серве-ре, на котором не работают никакие другие приложения (поэтому он может быть особенно надежно защищен от нападения; кроме того, этот сервер может быть сделан «невидимым» для нападающего). Для защиты сети устанавливаются несколько таких серверов, которые анализируют сетевой трафик в различных сегментах сети. Таким образом, несколько удачно расположенных систем могут контролировать большую сеть.

К недостаткам таких систем относят проблемы распознавания нападений в момент высокой загрузки сети, и неспособность анализировать степень проникновения (система просто сообщает об инициированном нападении).

2. СОВ, защищающие отдельный сервер. Собирают и анализируют информацию о процессах, происходящих на конкретном сервере. Благодаря узкой направленности, могут проводить высоко детализированный анализ и точно определять, кто из пользователей выполняет злонамеренные действия. Некоторые СОВ этого класса могут управлять груп-пой серверов, подготавливая централизованные обобщающие отчеты о возможных напа-дениях. В отличие от предыдущих систем могут работать даже в сети, использующей шифрование данных (когда информация находится в открытом виде на сервере до ее от-правки потребителю). Однако систем этого класса не способны контролировать ситуацию во всей сети, так как видят только пакеты, получаемые «своим» сервером. Кроме того, снижается эффективность работы сервера вследствие использования его вычислительных ресурсов.

3. СОВ на основе защиты приложений. Контролируют события, проявляющиеся в пределах отдельного приложения. Знания о приложении, а также возможность анализировать его системный журнал и взаимодействовать с ним посредством API, позволяет таким системам контролировать деятельность пользователей (работающих с данным приложением) с очень высокой степенью детализации.

Аналогично антивирусным программам, системы обнаружения вторжений используют два основных подхода к методам обнаружения подозрительной активности. Подход на основе сигнатуры выявляет деятельность, которая соответствует предопределенному набору событий, уникально описывающиему известное нападение. Эта методика чрезвычайно эффективна и является основным методом, используемым в коммерческих про-граммах. Однако, такая СОВ не может бороться с новыми видами нападений, а также с видоизмененными вариантами традиционных нападений, сигнатура которых незначительно отличается от имеющейся в базе. СОВ на основе аномалий обнаруживают нападения, идентифицируя необычное поведение на сервере или в сети. Они способны обнаруживать нападения, заранее не запрограмированные в них, но производят большое количество ложных срабатываний.

**Примерный список вопросов к зачету.**

1. Понятие "информационные технологии". Требования по защите информации: Классификация ОВТ от НСД.

2. Понятие "информационные процессы". Требования по защите информации: Классификация АС от НСД.

3. Перечислите методы поиска информации. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС.

4. Понятие "информационная система". Требования по защите информации: Классификация Межсетевых экранов.

5. Виды информации. Классификация ПО по отсутствию НДВ.

6. Защита информации. Основные термины и определения (защита информации, информационная система, информационно-телекоммуникационная сеть, обладатель информации, документированная информация, конфиденциальность информации).

7. Схема канала связи. Классификация угроз по способу доступа к ресурсам АС.

8. Виды информации ограниченного доступа. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных.

9. Дать определения следующим терминам. Автоматизированная система, автоматизированная информационная система, автоматизированная банковская система, банковский технологический процесс.

10. Приведите примеры инцидентов информационной безопасности.

11. Понятие инцидента информационной безопасности по ГОСТ ИСО/МЭК 13335-1 и инцидента информационной безопасности организации банковской системы РФ.

12. Модель угроз. Основные понятия (источник угроз, злоумышленник, уязвимость, ущерб.

13. Понятие риска и виды рисков.

14. Риск. Основные термины и определения (информационный риск (ИТ - риск) , операционный риск, менеджмент риска, остаточный риск, анализ риска, Оценка риска)

15. Какие задачи решает система обеспечения безопасности?

16. Понятие системы комплексной безопасности.

17. Свойства информации (доступность, целостность, конфиденциальность) .

18. Понятия государственной тайны, коммерческой тайны.

19. Система менеджмента (управления – в некоторых документах) информационной безопасности организации банковской системы Российской Федерации (определения, исходные данные, результаты деятельности).

20. Политика информационной безопасности. Определение и содержание.

21. Содержание интересов личности, общества и государства в информационной сфере.

22. Угрозы и источники угроз в информационной сфере Российской Федерации.

23. Источники угроз. Описание каждого вида.

24. Структура государственной системы информационной безопасности.

25. Федеральная служба по техническому и экспортному контролю (ФСТЭК России). Опишите функции, основные задачи.

26. Министерство обороны (Минобороны России). Опишите функции, основные задачи.

27. Для чего создается государственная система обеспечения информационной безопасности? Предпосылки появления угроз.

28. Мероприятия по реализации государственной политики обеспечения информационной безопасности РФ.

29. Классификация нормативной правовой информации по видам актов.

30. Доктрина информационной безопасности Российской Федерации. Основное содержание, общие положения.

31. Гражданский кодекс Российской Федерации. Статья 138, статья 139, статья 771, статья 857.

32. Национальные интересы РФ и стратегические национальные приоритеты.

33. Понятие, сущность и виды защищаемой информации.

34. Права и обязанности обладателя информации.

35. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит.

36. Основные факторы влияющие на состояние ИБ РФ.

37. Основные объекты ИБ РФ.

38. Особенности обеспечения ИБ в оборонной сфере.

39. Особенности обеспечения ИБ в общегосударственных информационных системах.

40. Способы воздействия угроз на объекты ИБ РФ.

41. Особенности обеспечения ИБ в сфере экономики.

42. Особенности обеспечения ИБ в общегосударственных телекоммуникационных системах.

43. Федеральный закон от 8 августа 2001 г. № 128-ФЗ "О лицензировании отдельных видов деятельности". Основное содержание, общие положения.

44. Постановление Правительства от 29 декабря 2007 г. N 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами». Основное содержание, общие положения. Термины и определения.

45. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании". Основное содержание, общие положения. Термины и определения.

46. Федеральный закон от 29 июля 2004 г. № 98-ФЗ "О коммерческой тайне". Основное содержание, общие положения. Термины и определения.

47. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 "О государственной тайне" (с изменениями и дополнениями). Основное содержание, общие положения. Термины и определения.

48. Федеральный закон от 7 июля 2003 г. № 126-ФЗ "О связи" (с изменениями и дополнениями). Основное содержание, общие положения. Термины и определения.

49. Федеральный закон от 7 августа 2001 г. № 119-ФЗ "Об аудиторской деятельности" (с изменениями и дополнениями). Основное содержание, общие положения. Термины и определения.

50. Федеральный закон от 27 июля 2006 г. № 149-ФЗ. "Об информации, информационных технологиях и о защите информации". Основное содержание, общие положения. Термины и определения.

51. Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ “О персональных данных”. Основное содержание, общие положения. Термины и определения.

52. Постановление Правительства РФ от 17 ноября 2007 г. N 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Основное содержание, общие положения. Термины и определения.

53. Нормативные документы и инструктивные материалы ФСТЭК (Гостехкомиссии) РФ.

54. Критерии безопасности компьютерных систем Министерства обороны США – "Оранжевая книга". Основное содержание, общие положения. Термины и определения.

55. Классы защищенности в соответствии с "Оранжевой книгой" .

56. Режимы функционирования в соответствии с "Оранжевой книгой" .

57.Цели Федеральных критериев безопасности информационных технологий

58. Понятие продукта ИТ.

59. Понятие профиля защиты.

60. Общие критерии безопасности информационных технологий. Основное содержание, общие положения. Термины и определения.

61. Общие критерии разрабатывались в расчете на то, чтобы удовлетворить запросы трех групп специалистов. Опишите эти группы.

62. ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий". Основное содержание, общие положения. Термины и определения.

63. Функциональные требования безопасности.

64. Руководящие документы Гостехкомиссии (ФСТЭК) России.

65. Сервисы безопасности и исполняемые ими роли

66. Сетевые механизмы безопасности.

67. Администрирование средств безопасности.

68. Обязанности администратора механизмов безопасности.

69. Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью — Информационные технологии». Основное содержание, общие положения. Термины и определения.

70. Германский стандарт BSI. Основное содержание, общие положения. Термины и определения.

71. Стандарты информационной безопасности в Интернете.

72. Перечислите примеры уязвимостей .

73. Уязвимости внешней среды и инфраструктуры.

74. Уязвимости аппаратных средств.

75. Уязвимости программные средств.

76. Уязвимости системы связи.

77. Информационные угрозы реализуются в виде.

78. Физические угрозы реализуются в виде.

79. Программно-математические угрозы реализуются в виде.

80. РД. Концепция защиты средств вычислительной техники в АС от НСД к информации. Основное содержание, общие положения. Термины и определения.

81. Технические каналы утечки информации.

82. Акустический и оптико-электронный канал утечки информации.

83. Оптический и вибро-акустический канал утечки.

84. Системы обнаружения вторжений (IDS).

85. Средства защиты сети. Межсетевые экраны

86. Способы атаки на пароль. Обеспечение безопасности пароля

87. Способы атаки на пароль. Полный перебор.

88. Способы атаки на пароль. Перебор в ограниченном диапазоне.

89. Способы атаки на пароль. Атака по словарю. Фишинг.

90. Способы атаки на пароль. Атака по персональному словарю

91. Компьютерные вирусы и борьба с ними

92. Общие сведения о компьютерных вирусах.

93. Классификация вирусов. Файловые вирусы.

94. Классификация вирусов. Макровирусы.

95. Классификация вирусов. Сетевые черви

96. Классификация вирусов. Загрузочные вирусы

97. Классификация вирусов. Троянские кони

98. Технологии маскировки вирусов. ВТСС - функциональное назначение.

99. Классификация каналов несанкционированного получения информации.

100. (КНПИ). ОТСС - функциональное назначение.

101. Структура технического канала утечки информации. Классификация технических каналов утечки информации.

**Вопросы, которые студенты должны подготовить самостоятельно (семинары).**

102. Государство как основной администратор в области защиты информации.

103. Государственные органы, уполномоченные защищать информацию.

104. Процесс получения разрешения на использование определённой информации.

105. Органы, правомочные запрещать определённые виды поведения в информационной сфере.

106. Роль и место экономической безопасности в системе национальной безопасности РФ.

107. Основные подходы к определению содержания понятия «экономическая безопасность».

108 Уровни экономической безопасности государства.

110. Объект и предмет экономической безопасности.

111. Экономическая политика государства и государственная стратегия обеспечения экономической безопасности России.

112. Зарубежный опыт обеспечения экономический безопасности.

113. Основные направления деятельности Межведомственной комиссии по безопасности в сфере экономики Совета Безопасности РФ.

114. Экономические интересы и приоритеты РФ.

115. Основные тенденции современного экономического развития России.

116. Макро и микроэкономические параметры как показатели экономической безопасности.

117. Экономический потенциал и национальное богатство страны.

118. Возможность использования государственного стратегического управления при обеспечении экономической безопасности.

119. Ответственность за нарушения в сфере информационной безопасности.

120. Понятие, методы защиты информации. Уровни защиты информации;

122. Угрозы информационным системам и их виды. Методы защиты информации;

123. Система защиты информации. Техническое обеспечение информационной безопасности. Информационное оружие.

124. Компьютерные преступления (киберпреступность). Методы киберпреследований.

125. Признаки незаконного проникновения в компьютерную систему. Дальнейшие действия в случае обнаружения незаконного проникновения в компьютерную систему.

126. Применение информационных технологий при организации защиты персональных данных.

127. Система электронного документооборота: понятия, принципы, классификация;

128. Электронный документооборот. Электронная цифровая подпись. Понятие информационных процессов и их виды;

130. Система управления документами. Сервисы. Управление записями: понятия, практика;

131. Понятие справочно-правовых систем (СПС) как специализированного класса информационных систем.

132. Влияние СПС на нормотворческую и правоприменительную деятельность. Роль СПС в повышении уровня правовой культуры и в правотворчестве.

133. Механизм пополнения справочно-правовых систем нормативными правовыми актами.

134. Понятие электронного правосудия: предназначение, решаемые задачи, виртуальная основа. Перспективы развития (Интернет-суды и т. п.).

135.Меры, применяемые государством в борьбе с преступлениями в сфере высоких технологий.

**Литература**

1. Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике. – М.: ИЛ, 1963.
2. Jackson K., Hruska J. (Ed.) Computer Security Reference Book. Butterworth-Heinemann Ltd., 2014. - 932 pp.
3. Muftic S. Security Mechanisms for Computer Networks. Halsted Press. Русский перевод: Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 2018.
4. Спесивцев А.В., Вегнер В.А. и др. Защита информации в персональных ЭВМ.- М.: Радио и связь, 2019.- 191 стр.
5. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. –М.: Яхтсмен, 2018.- 188 c.
6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоатомиздат, 2018, Кн. 1 и 2.
7. Михайлов С.Ф., Петров В.А., Тимофеев Ю.А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции. Учеб. пособие. - М.: МИФИ, 2018.- 112 с.
8. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. Учебное пособие. - М.: МИФИ, 2018.
9. Schneier B. Applied cryptography, second edition: protocols, algorithms, and source code in C. J. Wiley & sons, Inc. 2016.- 758 pp. Русский перевод: Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Триумф, 2018. – 816 с.
10. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 2019г., - 538 с.
11. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. – СПб.: НПО Мир и семья, 2019.
12. Торoкин А.А. Oснoвы инженернo-техническoй защиты инфoрмации. – М.: Ocь-89, 2019.-336 c.
13. Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. – СПб: СПбГУ, 2019. – 328 с.
14. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.:Радио и связь, 2019. – 328 с.
15. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб: СПбГУ, 2018. – 368 с.
16. 20. Stallings W. Network and Internetwork Security: principles and practice, Second Edition, Prentice-Hall, Inc., 2018.- 459 pp. Русский перевод: Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2019. – 672 с.
17. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю., Теоретические основы компьютерной безопасности, – М: Радио и связь, 2000. -192 с.
18. Зегжда Д., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телекомю 2018. – 452 с.
19. Милославская Н.Г., Толстой А.И. Интрасети:доступ в Internet, защита: Учебное пособие. – М.: ЮНИТИ-ДАНА, 2000. – 527 с.
20. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах, – М: Радио и связь, 2000. -168 с.
21. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. М.: СИНТЕГ, 2000, -248 с.
22. Ярочкин В.И. Информационная безопасность. – М.: Международные отношения, 2000г., - 400 с.
23. Безопасность сети на основе Windows 2000. Учебный курс MCSE. – М.: ИТД Русская Редакция. 2001. –912 с.
24. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРБ, 2001. –480 с.
25. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия-телеком, 2019г.,-148 с.
26. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. – М.: Юрист, 2019 г., - 415 с.
27. Стрельцов А.А. Обеспечение информационной безопасности России. - М.: МЦНМО, 2018.-296.
28. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2019. – 432 с.
29. Barman S. Writing Information Security Policies. 2011.Русский перевод: Бармен С. Разработка правил информационной безопасности. – М.: Вильямс, 2018.- 208 с.
30. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб.: Питер, 2018. – 848 с.
31. Smith R. Authenticaton: From Passwords to Public Keys. – NY: Addison-Wesley Publishing Company, Inc., 2018. Русский перевод: Смит Р. Аутентификация: от паролей до открытых ключей. – М.: Вильямс, 2018. – 432 с.
32. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. Учеб. пособие. –М.: РГГУ, 2018.-399 с.
33. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учеб. пособие. – М.: Радио и связь. 2017.- 296 с.
34. Конеев И., Беляев А. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2017.-752с.
35. Скляров Д.В., Искусство защиты и взлома информации.- СПб.: БХВ - Петербург, 2018.-288 c.
36. Галатенко В.А. Стандарты информационной безопасности. Курс лекций. М.: ИНТУИТ. РУ, 2018. – 328 с.
37. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности: Учебное пособие. – М.: Гелиос АРВ, 2018.- 144 с.
38. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография.- М.: Норма, 2018. – 432 с.
39. Гринберг А.С., Горбачев Н.Н., Бондаренко А.С. Информационные технологии управления: Учеб. Пособие для вузов. – М.: ЮНИТИ - ДАНА, 2018.-479с.(8.10. Технологии обеспечения информационной безопасности. 358-371стр.)
40. Государственная тайна и ее защита. Собрание законодательных и нормативных правовых актов. – М.: «Ось-89», 2018.-160 с.
41. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М., Белов Е.Б., Полникова С.В. Правовое обеспечение информационной безопасности: Учеб. пособие.- М.: Издательский центр «Академия», 2015.-240 с.
42. Информационные технологии управления: Учеб. Пособие для вузов/ Под ред.проф. Г.А. Титоренко. – М.: ЮНИТИ-ДАНА, 2015.-439с. (6. Защита информации в ИС и ИТ управления организацией, 192-221 стр.)
43. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособие. – М.: Гелиос АРВ, 2015.- 192 с.
44. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск.: БЕЛЛIТФОНД, 2015.-304 с.
45. Венбо Мао. Современная криптография: теория и практика.: Пер. с англ.- М.: Вильямс, 2015. 768 c.
46. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная информация. Компания АйТи; ДМК Пресс, 2015.-384 c.
47. Фисун А.П., Касилов А.Н., Глоба Ю.А., Савин В.И., Белевская ю.А. Право и информационная безопасность: Учебное пособие// -М.: Приор-издат, 2015.-272 с.
48. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: Учеб. пособие. – М.: Гелиос АРВ, 2015.- 224 с.
49. Асанович В.Я., Маньшин Г.Г. Информационная безопасность: анализ и прогноз информационного взаимодействия. – Мн.: Амалфея, 2016.-204 с.
50. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2018.- 544 с.
51. Филин С.А. Информационная безопасность: Уч. Пособие. - М.: Альфа-Пресс, 2018.-412с.
52. Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи, 2018. – 400 с.
53. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем: Уч. Для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая линия – Телеком, 2018. – 536 с.
54. Галатенко В.А. Основы информационной безопасности. Курс лекций. - М.: ИНТУИТ. РУ, 2018г. – 205 с.
55. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие. – М.: ФОРУМ: ИНФРА-М. 2018. – 368 с.
56. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учеб. пособие. – М.: Гелиос АРВ, 2018.- 528 стр.
57. Сердюк В.А. Новое в защите от взлома корпоративных систем. М.: Техносфера, 2019.- 360 с.
58. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебн. Пособие.- М.: ИД «ФОРУМ»: ИНФРА-М,2018.-416 с.
59. ТИИЭР т.76, №5. Защита информации. Малый тематический выпуск. – М.: Мир, 1988.
60. Garfinkel S. PGP: Pretly Good Privacy. – O’Reilly and Associates, Inc., 2015
61. Hoffman L. (Ed.) Building in big Brother: the cryptography policy debate. Springer-Verlag NewYork. Inc. , 2018- 560 pp.
62. Kaufman C., Pelman R., Speciner M. Network Security – PRIVATE Communication in a PUBLIC World, Prentice-Hall, Inc.,1995.
63. Варфоломеев А.А., Пеленицин М.Б. Методы криптографии и их применение в банковских технологиях. – М.: МИФИ, 2018.- 116 стр.
64. Варфоломеев А.А., Гаврилкевич М.В., Устюжанин Д.Д., Фомичев В.М. Методические указания к выполнению лабораторного практикума “Информационная безопасность. Криптографические методы защиты информации”, ч.1 ,ч.2. – М.: МИФИ, 2015. – 44 с., - 38с.
65. Menezes A., Van Oorschot P., Vanstone S. Handbook of Applied cryptography. CRC Press, 2018.- 816 стр.
66. Теория и практика обеспечения информационной безопасности. Под ред. Зегжды П.Д. – М.: Яхтсмен, 2018.
67. Анин Б. Защита компьютерной информации. – СПб.: БХВ-Санкт-Петербург, 2018.- 384 с.
68. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.:ДМК, 2018. – 448 с.
69. Burnet S., Paine S. RSA Security`s Official Guide to Cryptography.- NY.: The McGraw-Hill Companies, 2017. Русский перевод: Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security.- М.: Бином-Пресс, 2017. –384 с.
70. Голдовский И. Безопасность платежей в Интернете. – СПб : Питер, 2017. – 240 с.
71. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. – Мн.:БГУ, 2018. – 190 с.
72. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий. \_ М.: Издательство СИП РИА, 2018. – 356 с.
73. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер. – М.: Гелиос АРБ, 2017. – 256 с.
74. Парфенов В.И. Защита информации. Словарь. Воронеж.: НП РЦИБ Факел. 2017, - 292 с.
75. Царегородцев А.В. Информационная безопасность в распределенных управляющих системах. – М.: РУДН, 2017.
76. Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2017.- 192 с.
77. Максим М., Полино Д. Безопасность беспроводных сетей. – М.: Компания АйТи, ДМК Пресс, 2018. – 288 с.(пер. книги 2016 изд.)
78. Смарт Н. Криптография. М.: Техносфера, 2015.- 528 с.
79. Земор Ж. Курс криптографии.- М.-Ижевск: НИЦ”Регулярная и хаотическая динамика”; Институт компьютерных исследований, 2018.-256
80. Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.; Мир, 2018, 471 с.
81. Зубов А.Ю. Математика кодов аутентификации. – М.: Гелиос АРБ, 2017.- 480с.
82. Доля А.А. Внутренние ИТ - угрозы в России – 2016. «Защита информации. Инсайд», №2 март-апрель 2017. 60-69 стр.